Instalación y seguridad en eGroupWare

Versión 0.4

Este documento está publicado bajo la
Creative Commons Attribution-ShareAlike License

Las extensiones y respuestas a este documento son bienvenidas
Por favor, póngase en contacto con el autor

Autor: Reiner Jung
Copyright: Reiner Jung
Contacto: r.jung@creativix.net
Coordinador traducción español: Oscar Manuel Gómez Senovilla
Contacto: omgs@users.sourceforge.net

Proyecto: eGroupWare
Fecha de publicación: 8 de agosto de 2004

Indice

Indice 3
1 Elementos necesarios para la instalación de eGroupWare 6
2 Método rápido de instalación 7
3 Migrar una instalación de phpGroupWare a eGroupWare 12
4 Actualizar eGroupWare 13
4.1 Actualizar la instalación de eGroupWare 13
4.2 Portar la configuración a la nueva versión de header.inc.php 13
5 Pasos necesarios para instalar eGroupWare 14
5.1 Descargar los paquetes 14
5.2 ¿Por qué son necesarias las firmas gpg y md5sum? 14
5.2.1 Instale la clave GPG para tar.gz.gpg, tar.bz2.gpg y zip.gpg 14
5.2.2 Comprobar la clave GPG 14
5.2.3 Instale la clave GPG para los paquetes rpm 16
5.3 ¿Cómo puedo validar los paquetes? 16
5.4 Instalar los paquetes en el servidor 18
5.4.1 Rehacer los paquetes para otras rutas 18
5.4.2 Instalar un paquete sin firmar en el servidor 18
5.4.3 Instalar un paquete con firma gpg en el servidor 18
5.4.4 Instalar desde CVS 19
6 Seguridad básica del servidor 20
6.1 La plataforma del servidor 20
6.1.1 Comprobar los servicios que se ejecutan y puertos abiertos 20
6.1.1.1 Puertos que el servidor eGroupWare necesita para su ejecución 20
6.1.1.2 El escaneador de puertos 21
6.1.1.3 Salida de un escaneador de puertos 21
6.1.1.4 Desactivar servicios que no se necesitan 21
6.1.2 Desinstalar programas que no se necesitan en el servidor 22
6.1.3 Comprobación local de existencia de un rootkit 22
6.1.3.1 Fragmento de ejemplo de chkrootkit 23
6.1.3.2 Instalar el rpm de chkrootkit 23
6.1.3.3 Instalar chkrootkit desde un tar.gz 23
6.1.4 Administradión de un servidor seguro 24
6.1.4.1 Conéctese a su servidor con una sesión segura 24
6.1.4.2 Trabajando con pares de claves SSH 25
6.1.4.2.1 Crear un par de claves seguras 25
6.1.4.2.2 Copiar la clave pública al servidor 26
6.1.4.2.3 La herramienta ssh-add 26
6.1.4.2.4 Seguridad en su cliente SSH 26
6.1.4.2.5 Seguridad en el servidor SSHD 26
6.1.5 Instalar software para monitorizar los registros del sistema 27
6.1.6 Entorno de detección de intrusos 27

6.1.6.1 Instalación de Aide 28
6.1.6.2 El fichero de configuración de Aide, aide.conf 28
6.1.6.3 Crear un fichero cron para ejecutar Aide automáticamente 30
6.1.6.4 Informe de ejemplo de AIDE 32
6.1.6.5 Crear una base de datos nueva después de los cambios 33
6.1.7 Seguridad de los servicios en demonios 33
6.1.8 Cortafuegos 33
6.2 Seguridad en aplicaciones web 33
6.2.1 Instalar ModSecurity 33
6.2.2 Configuración básica 34
6.2.3 Comprobar ModSecurity 35
6.2.4 Registro de ejemplo de ModSecurity 35
6.3 Optimización y seguridad en Apache 37
6.3.1 Módulos recomendados 37
6.3.2 Otras opciones de configuración de Apache 37
6.4 Turck MMCache 37
6.4.1 Requisitos 38
6.4.1.1 Tareas previas en RedHat Enterprise Linux 3 38
6.4.2 Compatibilidad 39
6.4.3 Instalación rápida 39
6.4.4 Interfaz web 40
6.5 Seguridad de la instalación PHP 41
6.6 Crear un certificado para el servidor web 42
6.6.1 Unirse a una Autoridad de certificación (CA) 43
6.6.2 Crear una solicitud de firma de certificado 43
6.6.2.1 Cambiar el fichero openssl.cnf 43
6.6.2.2 Crear la clave de servidor y solicitud de firma 44
6.6.2.3 Enviar la solicitud de firma a la CA 45
6.6.2.4 Instalar el certificado en el servidor 45
6.7 El servidor web 46
6.8 El servidor de bases de datos SQL 46
7 Instalación de eGroupWare 47
7.1 Crear la base de datos 47
7.2 ¿Cómo iniciar la configuración? 48
7.3 Comprobar la instalación de eGroupWare 48
7.4 Crear el fichero header.inc.php 49
7.5 Administrador de instalación/configuración 50
7.5.1 Paso 1 Gestión simple de aplicaciones 50
7.5.2 Paso 2 - Configuración 51
7.5.2.1 Crear el directorio para los ficheros 51
7.5.2.2 Editar la configuración actual 52
7.5.3 Paso 3 – Configurar las cuentas de los usuarios 54
7.5.4 Paso 4 – Administrar idiomas 55
7.5.5 Paso 5 – Administrar aplicaciones 55
8 Iniciar una sesion en eGroupWare 55

9 Resolución de problemas 56
9.1 Olvido de la contraseña de administrador 56
9.2 El usuario administrador u otro usuario está bloqueado 56
9.3 Database error: lock(Array, write) failed 56
9.4 Comprobar los permisos de los ficheros 56
9.5 No puedo pasar de la página de Comprobar la instalación (1) 57
9.6 No puedo pasar de la página de Comprobar la instalación (2) 57
9.7 [WINDOWS] fudforum/3814******9): Permiso denegado 57
9.8 Sitemgr: mkdir(./sitemgr-link): Permiso denegado 58
10 Mapa de Software 59
11 Tareas pendientes y registro de cambios 62
11.1 La lista de tareas pendientes de este documento 62
11.2 Registro de cambios para este documento 62
12 Colaboradores en este documento 63
13 Licencia legible por humanos 65

1 Elementos necesarios para la instalación de eGroupWare

Esta lista tiene como objetivo proporcionar una breve descripción de lo que se necesita para ejecutar eGroupWare.
No es necesario ningún compilador para instalar eGroupWare, que está compuesto sólo por PHP, HTML y ficheros de imágenes.

Lo que necesita para ejecutar eGroupWare	Software ejemplo	Marcar los requisitos
Se necesita un sistema operativo como los siguientes	Linux, Unix, *BSD MAC WIN NT / 2000 / XP	☑ ☐ ☒ ☐
eGroupWare requiere un servidor web. Algunos ejemplos son:	IIS Roxen Apache 1.3 o 2.0	☑ ☐ ☒ ☐
eGroupWare requiere una base de datos.	MYSQL MS-SQL PostgreSQL	☑ ☐ ☒ ☐
Si se quiere enviar correo con eGroupWare, entonces se necesita un servidor SMTP	Postfix Sendmail Exim …	☑ ☐ ☒ ☐
Si se quiere usar eGroupWare como un cliente de correo POP o IMAP, se necesita tener acceso a un servidor externo:	Cyrus Courier Dovecot	☑ ☐ ☒ ☐
eGroupWare requiere PHP	PHP > 4.1 requerido. Se recomienda PHP > 4.2	☑ ☐ ☒ ☐

2 Método rápido de instalación

Este método le dará una breve introducción sobre los pasos a seguir para configurar eGroupWare. Una instalación de eGroupWare se puede hacer en menos de 10 minutos. Si desea tener una descripción más detallada acerca de la instalación y la seguridad, lea las siguientes páginas de este método rápido de instalación.

1) Descargue los paquetes de eGroupWare desde el área de descarga de ourceforge
En este instante, eGroupWare está disponible en formato zip. tar.gz, bz2 y rpm.

2) [LINUX] Instale los paquetes en el servidor en el raíz del servidor web un otro directorio que quiera usar. El paquete RPM se instalará automáticamente en el directorio /var/www/html

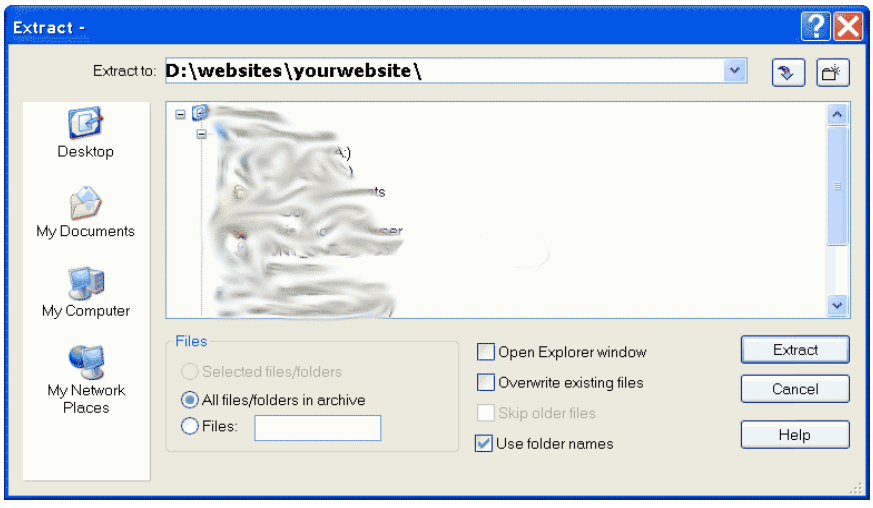
```
[root@server tmp]# rpm –ivh eGroupWare-x.x.xx.xxx-x.rpm
```

Para instalar otro paquete desde eGroupWare, descomprímalo desde el directorio raíz del servidor web donde haya instalado la aplicación

```
[root@server tmp]# cd /var/www
[root@server www]#tar xzvf eGroupWare-x.x.xx.xxx-x.tar.gz
```

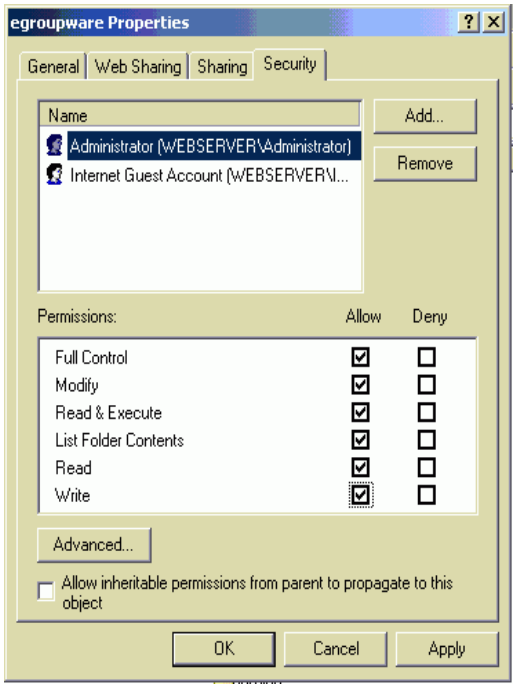
[WINDOWS] Usando un programa como Winzip, descomprima el fichero a cualquier directorio que esté debajo del servidor web. En otras palabras, el directorio elegido debe ser accesible desde Internet.

Asegúrese de que guarda la estructura de directorios existente al extraer el fichero zip, y la instalación estará en un directorio similar a D:\websites\yourwebsite\eGroupware\(todos los ficheros en el zip de eGroupware).

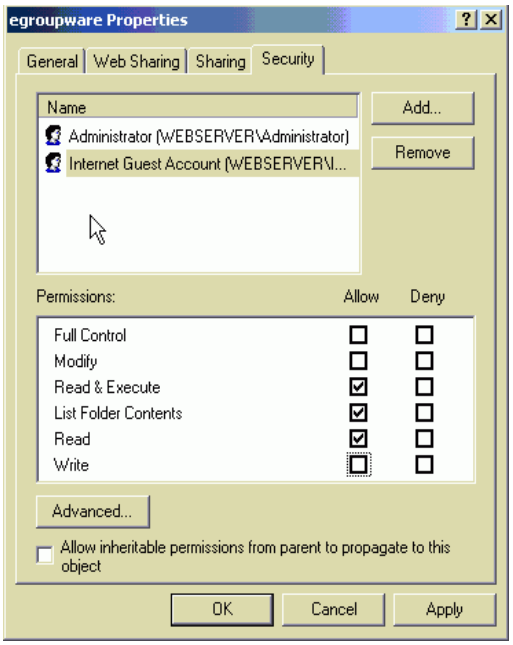


3) [LINUX] Cambie los permisos de los ficheros de la instalación de eGroupWare
   - El administrador debe tener derechos para leer y escribir
   - El usuario del sistema con el que se ejecuta el servidor web debe tener permisos sólo de lectura
     Sólo para el directorio fudforum, el servidor web necesita tener derechos de escritura

[WINDOWS] Ahora debe establecer los permisos adecuados para los ficheros de eGroupware.



El usuario Administrativo necesita tener al menos permisos de **lectura** and **escritura**.



El usuario Web necesita tener permiso de lectura.

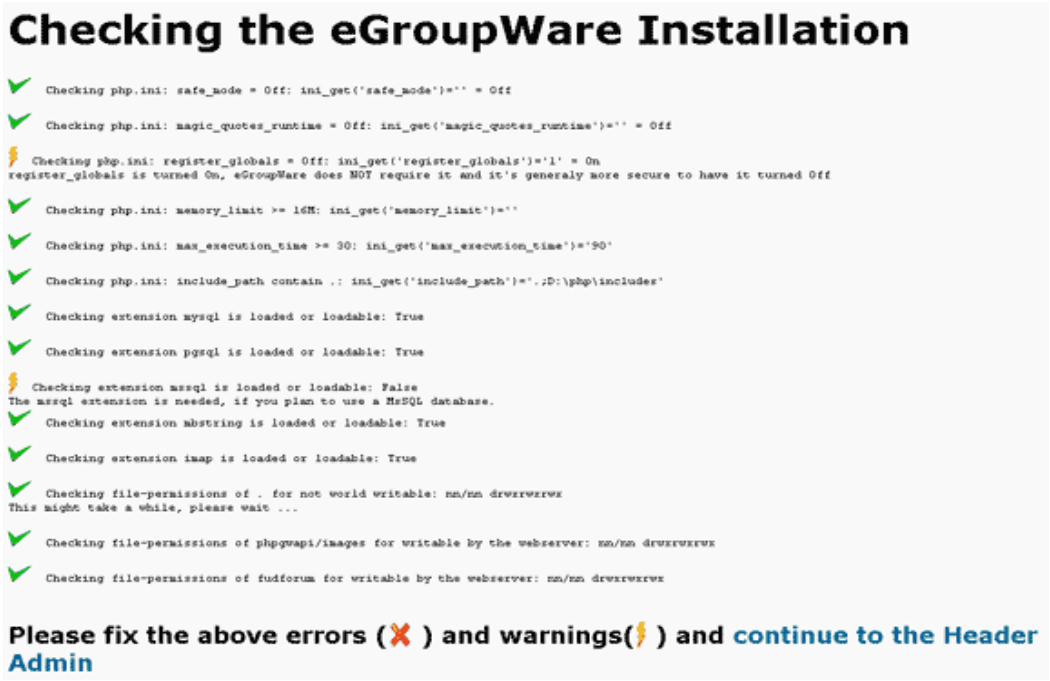
Para FUDFORUM solamente – El usuario Web necesita tener permisos de lectura y escritura

4) Asegúrese de que se están ejecutando el servidor web y la base de datos.

5) Introduzca en el navegador la URL correspondiente a la instalación
http://servidor/egroupware/setup

6) El script de comprobación de la instalación se iniciará automáticamente.
- Espere hasta que el script acabe, y corrija los errores que se muestren
- Después de corregir los errores, recargue la página para volver a comprobar la instalación
- Cuando ya no haya errores, desplácese hacia abajo y pulse Volver a la instalación

[WINDOWS] Puede que haya un par de cosas que no se resuelvan completamente. Por ejemplo, la configuración de register_globals = on en el fichero PHP.ini (normalmente en C:\WINNT). Algunos scripts requieren que está opción esté en on y algunos necesitan que esté en off. Si lo desactiva, algún sitio que tenga definido podría no funcionar. La forma de asegurarse es la que eGroupware recomienda (off) y comprobar los otros sitios. Si no funcionan, entonces vuelva a dejarl register_globals = on. Por favor, tenga en cuenta que eGroupWare not requiere que esté en (off)! Tampoco se cargará la extensión de la base de datos MsSQL (Microsoft) si está usando MySQL.


Checking the eGroupWare Installation
Checking php.ini: safe_mode = Off: ini_get('safe_mode')='' = Off
Checking php.ini: magic_quotes_runtime = Off: ini_get('magic_quotes_runtime')='' = Off
Checking php.ini: register_globals = Off: ini_get('register_globals')='1' = On
register_globals is turned On, eGroupWare does NOT require it and it's generaly more secure to have it turned Off
Checking php.ini: memory_limit >= 16M: ini_get('memory_limit')=''
Checking php.ini: max_execution_time >= 30: ini_get('max_execution_time')='90'
Checking php.ini: include_path contain .: ini_get('include_path')='.;D:\php\includes'
Checking extension mysql is loaded or loadable: True
Checking extension pgsql is loaded or loadable: True
Checking extension mssql is loaded or loadable: False
The mssql extension is needed, if you plan to use a MsSQL database.
Checking extension mbstring is loaded or loadable: True
Checking extension imap is loaded or loadable: True
Checking file-permissions of . for not world writable: nn/nn drwxrwxrwx
This might take a while, please wait ...
Checking file-permissions of phpgwapi/images for writable by the webserver: nn/nn drwxrwxrwx
Checking file-permissions of fudforum for writable by the webserver: nn/nn drwxrwxrwx
Please fix the above errors ( ) and warnings( ) and continue to the Header Admin

Cuando haya resuelto los conflictos, pulse en "continue to the Header Admin"

7) La configuración para el inicio del administrador de encabezados
- Rellene todos los campos

[WINDOWS] Server Root – Este valor es el directorio "raíz" de la instalación de eGroupware en el disco duro. Por ejemplo: D:\websites\yourwebsite\egroupware
Include Root – normalmente tiene el mismo valor que "Server Root" (Nota: no es la dirección de internet, sino el directorio actual a la instalación de eGroupWare.
- Descargue el fichero header.inc.php y guárdelo en el directorio raíz de la instalación de eGoupWare (por ejemplo /var/www/html/egroupware). De al servidor web permiso de lectura en

el fichero.
- Pulse continue

[WINDOWS] Elija la opción "Download" (descargar) el fichero header.inc.php que acaba de crear, y guárdelo en el directorio raíz de la instalación de eGroupware (si tiene accesso al servidor), o súbalo por FTP al directorio indicado.

No olvide la contraseña. Se guardará en forma cifrada y no se puede leer después.

8) Entre en setup/Config Admin

9) Cree la base de datos y las tablas
- Rellene el formulario siguiente con la "contraseña de root de la base de datos y contraseña" para crear su base de datos automáticamente
- Continúe con la opción de crear de la base de datos
- Vuelva a comprobar la instalación
- Continúe con la opción crear tablas

[WINDOWS] Esto debería ser muy simple si conoce el nombre y la contraseña del servidor MySQL. Rellene la información y pulse en "Crear la base de datos"

Cuando pulse en "Volver a comprobar mi instalación", verá que "no tiene aplicaciones instaladas", y tendrá la opción de "instalar las tablas principales y las aplicaciones de preferencias de administración." Siga adelante e instale las tablas.
*Nota: Si hay errores, vaya a la sección "Resolución de problemas".

10) Editar configuración actual
- Cree un directorio fuera de la estructura del servidor web y otorgue permisos de lectura, escritura y ejecución para el servidor web.
Si la raíz de su servidor web server está bajo /var/www/html, puede crear el directorio, por ejemplo, en /var/www/files

[WINDOWS] Hay que crear un directorio que no esté por debajo de la instalación. Por ejemplo, si el raíz de la instalación es D:\websites\yourwebsite\eGroupware – el directorio podría ser algo como D:\websites\yourwebsite\nuevo_directorio. Una vez que el director esté creado, asegúrese de que el usuario del servidor Web tiene permisos de lectura, escritura y ejecución en este directorio.

11) Crear el usuario administrador
- No use este usuario en sus tareas normales. Este usuario sólo debe usarse como resguardo y para la configuración inicial

12) Administrar idiomas
- Instale los idiomas que desee usar

13) Administrar aplicaciones

- Desinstale las aplicaciones que no quiera usar

14) Inicie la sesión en eGroupWare

Pong en el navegador la url que corresponda a su instalación, http://servidor/egroupware

3 Migrar una instalación de phpGroupWare a eGroupWare

Descargue los paquetes necesarios de nuestra página como se describe en la sección 2.
Copie el fichero header.inc.php de su directorio de phpGroupWare al de eGroupWare y edite las siguientes líneas en el fichero header.inc.php:

De:

```
define('PHPGW_SERVER_ROOT','/var/www/html/phpgroupware');
define('PHPGW_INCLUDE_ROOT','/var/www/html/phpgroupware');
```

A:

```
define('PHPGW_SERVER_ROOT','/var/www/html/egroupware');
define('PHPGW_INCLUDE_ROOT','/var/www/html/egroupware');
```

Ponga en el navegador la URL correspondiente:

https://www.dominio.com/egroupware/setup

Inicie sesión en Setup/Config Admin Login

Pulse en Editar configuración actual

y cambie el contenido del tercer campo (Introduzca la ubicación...) a: /egroupware

Eso es todo. ¡Diviértase!

4 Actualizar eGroupWare

4.1 Actualizar la instalación de eGroupWare

1) Descargue los paquetes de la página en sourceforge.
2) Instale los paquetes en su servidor

   Para paquetes rpm, haga lo siguiente

   [root@server tmp]# rpm –Uvh eGroupWare*

   Para paquetes tar.gz, vaya al directorio raíz del servidor web (el directorio superior a la instalación de eGroupWare)

   [root@server tmp]# cd /var/www/html
   [root@server html]# tar xzvf eGroupWare-x.xx.xxx-x.tar.gz

   Para paquetes tar.bz2, vaya al directorio raíz del servidor web (el directorio superior a la instalación de

   [root@server tmp]# cd /var/www/html
   [root@server html]# tar xjvf eGroupWare-x.xx.xxx-x.tar.bz2

   Es posible actualizar desde CVS. AVISO: actualice desde CVS sólo desde la rama estable y no desde la rama de desarrollo.

   [root@server tmp]# cd /var/www/html/egroupware
   [root@server egroupware]# cvs update -Pd

3) Entre en Setup/Config Admin
4) Si es necesario, eGroupWare le mostrará que tiene que actualizar la base de datos
5) Compruebe las actualizaciones necesarios en el paso 4, Administración de aplicaciones avanzada

4.2 Portar la configuración a la nueva versión de header.inc.php

1) Después de la instalación, posiblemente verá el siguiente mensaje:
   Necesita portar su configuración a la nueva versión de header.inc.php.
2) Vaya a https://suservidor/egroupware/setup
   - Desplácese hacia abajo hasta "Comprobar la instalación de eGroupWare"
   - Confirme pulsando el botón Continue to the Header Admin
3) Introduzca su nombre de usuario y contraseña
4) Si es necesario, cambie la configuración
5) Guarde el fichero

5 Pasos necesarios para instalar eGroupWare

5.1 Descargar los paquetes

Se puede descargar el paquete de:
http://sourceforge.net/project/showfiles.php?group_id=78745

Proporcinamos los siguientes paquetes en el área de descargas de sourceforge.

*.tar.gz
*.tar.bz2
*.zip

Estos paqutes están firmados con una clave gpg por motivos de seguridad.

*.tar.gz.gpg
*.tar.bz2.gpg
*.zip.gpg

Estos rpms funcionan bajo RedHat y la mayoría de distribuciones basadas en rpm.

eGroupWare*noarch.rpm

El paquete eGroupWare-all-apps*.noarch.rpm contiene todos los paquetes disponibles.
Los otros paquetes proporcionan todas las aplicaciones en paquetes separados.

5.2 ¿Por qué son necesarias las firmas gpg y md5sum?

A veces, hackers maliciosos atacan servidores de desarrollo para cambiar los paqutes descargables, e incluir troyanos, sniffers, etc. en los paquetes. Los paquetes firmados sirven para comprobar la validez de la integridad de los paquetes del proyecto.

5.2.1 Instale la clave GPG para tar.gz.gpg, tar.bz2.gpg y zip.gpg

Instale la clave gpg con la que se han firmado los paquetes tar.gz.gpg, tar.bz2.gpg, zip.gpg, md5sum-eGroupWare-version.txt.asc y los rpms.

En Linux, se puede usar el siguiente comando para importar la clave que validar los paquetes tar.gz.gpg, tar.bz2.gpg, zip.gpg y md5sum*.asc.

```
[root@server root]# gpg --keyserver blackhole.pca.dfn.de --recv-keys 0xD9B2A6F2
```

5.2.2 Comprobar la clave GPG

Si quiere comprobar la validez de los paquetes, debe confiar en la clave. Si no hace esto, recibirá cada vez un mensaje de error diciendo que la clave no es de confianza.

Mire la lista de las claves disponibles en su anillo. Aquí debe ver la clave importada

```
[root@server root]# gpg --list-keys
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
/root/.gnupg/pubring.gpg
--------------------------------
pub  1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
sub  1024g/D08D986C 2002-12-22
```

Ahora, edite la clave con el identificador D9B2A6F2

```
[root@server root]# gpg --edit-key  D9B2A6F2
gpg (GnuPG) 1.0.7; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html for more information
gpg: checking the trustdb
gpg: no ultimately trusted keys found

pub  1024D/D9B2A6F2  created: 2002-12-22 expires: never      trust: -/-
sub  1024g/D08D986C  created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
```

Aunque no es necesario, puede comprobar también la huella digital de la clave. La huella de la clave es: BBFF 354E CA1F 051E 932D 70D5 0CC3 882C D9B2 A6F2

```
Command> fpr
pub  1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
          Fingerprint: BBFF 354E CA1F 051E 932D  70D5 0CC3 882C D9B2 A6F2
```

Ahora puede firmar la clave

```
Command>trust
pub  1024D/D9B2A6F2  created: 2002-12-22 expires: never      trust: f/-
sub  1024g/D08D986C  created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

 1 = Don't know
 2 = I do NOT trust
```

3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
i = please show me more information
m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? yes

pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never trust: u/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
Please note that the shown key validity is not necessary correct
unless you restart the program.

Now you can check the key at the prompt with "check" or quit the session.

5.2.3 Instale la clave GPG para los paquetes rpm

Para importar la clave que se necesita para validar los paquetes rpm, busque la clave D9B2A6F2 en el servidor de clave:
http://www.dfn-pca.de/eng/pgpkserv/

Pulse en el enlace D9B2A6F2 en la nueva ventana, y copie todo, incluyendo las siguientes líneas

----BEGIN PGP PUBLIC KEY BLOCK----
-----END PGP PUBLIC KEY BLOCK-----

y guarde el texto copiado en un fichero llamado:

EGROUPWARE-GPG-KEY

Como último paso, importe la clave en su anillo rpm:

```
[user@server tmp]$  rpm --import EGROUPWARE-GPG-KEY
```

5.3 ¿Cómo puedo validar los paquetes?

Si desea comprobar el md5sum de un paquete, realice las siguientes acciones:
En la línea de comando en su sistema Linux, introduzca las siguientes líneas:

Descargue el fichero md5sum-eGroupWare-version.txt.asc de la página de descargas de sourceforge
Compruebe la validez del fichero md5sum-eGroupWare-version.txt.asc

```
[user@server tmp]$ gpg --verify md5sum-eGroupWare-version.txt.asc
```

Averigüe el md5sum de un paquete

```
[user@server tmp]$ md5sum eGroupWare-x.x.xx.xxx-x.tar.gz
41bee8f27d7a04fb1c3db80105a78d03  eGroupWare-x.x.xx.xxx-x.tar.gz
```

y abra el fichero md5sum para ver el md5sum original (lo de debajo es sólo un ejemplo)

```
user@server tmp]$ less md5sum-eGroupWare-x.x.xx.xxx-x.txt.asc

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

md5sum from file eGroupWare-x.x.xx.xxx.tar.gz is:
41bee8f27d7a04fb1c3db80105a78d03
- ---------------------------------------

md5sum from file eGroupWare-x.x.xx.xxx.tar.bz2 is:
3c561e82996349d596540f476b9624f2
- ---------------------------------------

md5sum from file eGroupWare-x.x.xx.xxx.zip is:
c3bb1f67ca143236e8603c6995e82db0
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQE/WM2wDMOILNmypvIRAm5GAJ0e6IlnellZU0quVQxWOP/pF+QGpwCgptbH
O02LpinLNqnr6epxt9vB9sw=
=OBcn
-----END PGP SIGNATURE-----
```

Aquí vemos que la clave en el fichero md5sum y el test de checksum desde la línea de comando devuelven el mismo contenido, por lo que el paquete no fue modificado en el servidor después de crearlo.

Para comprobar el checksum de los tar.gz.gpg, tar.bz2.gpg o zip.gpg, siga estos pasos:
En la línea de comando de su sistema Linux, escriba las siguientes líneas:

```
[user@server tmp]$ gpg --verify eGroupWare-x.x.xx.xxx-x.tar.gz.gpg
```

Para comprobar el checksum del paquete rpm, siga estos pasos:
En la línea de comando de su sistema Linux, escriba las siguientes líneas:

```
[user@server tmp]$ rpm --checksig eGroupWare-all-apps-x.x.xx.xxx-x.noarch.rpm
```

5.4 Instalar los paquetes en el servidor

5.4.1 Rehacer los paquetes para otras rutas

Se pueden recompilar los paquetes para SuSE Linux. Por favor, descarge el src.rpm y escriba:

```
[user@server tmp]$ rpmbuild -–rebuild eGroupWare-x.xx.xxx-x.src.rpm
```

Esto creará un paquete con una ruta de instalación "/srv/www/htdocs"
El paquete se ubicará en el directorio /usr/src/packages/RPMS/noarch

5.4.2 Instalar un paquete sin firmar en el servidor

Para instalar un paquete rmp sin firmar, haga lo siguiente:

Vaya al directorio raíz del servidor web (o a donde quiera instalar los paquetes)

```
[user@server tmp]$ cd /var/www/html
```

Extraiga el paquete en este directorio. Si el paquete está en el directorio /tmp, puede instalarlo con

```
[user@server tmp]$ tar xzvf /tmp/eGroupWare-x.xx.xxx-x.tar.gz .

[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2 .

[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip .
```

5.4.3 Instalar un paquete con firma gpg en el servidor

Para instalar un paquete firmado que no es rpm, haga lo siguiente:

Separe el paquete de la clave gpg

```
[user@server tmp]$ gpg -o eGroupWare-X.XX.XXX-X.tar.gz -decrypt
eGroupWare-X.XX.XXX-X.tar.gz.gpg
```

Vaya al directorio raíz del servidor web (o donde quiera instalar los paquetes)

```
[user@server tmp]$ cd /var/www/html
```

Extraiga el paquete en este directorio. Por ejemplo, si el paquete está en el directorio /tmp, puede instalarlo con

```
[user@server html]$ tar xzvf /tmp/eGroupWare-x.x.xxx-x.tar.gz .

[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2 .
```

```
[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip
```

Instalar un paquete rpm en el servidor

Para instalar un paquete rpm, siga estos pasos:

Compruebe que el rpm es válido

```
[user@server tmp]$ rpm --checksig /tmp/eGroupWare-x.x.xxx-x.noarch.rpm
```

Instale el paquete

```
[user@server tmp]$ rpm -ivh /tmp/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm
```

Si la raíz del servidor web no es /var/www/html/, puede instalar el rpm en otro directorio. Para ello, use el siguiente comando.

```
[user@server tmp]$ rpm -ivh –prefix /your_new_server/root /tmp/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm
```

5.4.4 Instalar desde CVS

Para instalar los paquetes desde nuestro repository CVS, haga lo siguiente:

Vaya al directorio raíz del servidor web (o donde quiera instalar los paquetes)

```
[root@server tmp]# cd /var/www/html

[root@server html]# cvs –d:pserver:anonymous@cvs.sourceforge.net:
/cvsroot/egroupware login

[root@server html]# cvs –z3 –d:pserver:anonymous@cvs.sourceforge.net:
/cvsroot/egroupware co egroupware

[root@server html]# cd egroupware

[root@server egroupware]# cvs co all
[root@server egroupware]# cvs update -Pd
```

6 Seguridad básica del servidor

6.1 La plataforma del servidor

Puede elegir muchas posibilidades para tener seguridad en el servidor. La medida de seguridad más importante que se puede hacer es mantener la instalación actualizada. Para eGroupWare, puede suscribirse a la lista de correo egroupware-announcement@lists.sourceforge.net . Aquí publicamos las nuevas versiones y también las actualizaciones de seguridad necesarias de eGroupWare.

6.1.1 Comprobar los servicios que se ejecutan y puertos abiertos

Un puerto abierto significa que un servidor ofrece un servicio al público. Por ejemplo, este servicio público puede ser un servidor de ficheros, un servicio DNS, un servidor de telnet, un servidor X u otros servicios. El servidor debe tener abiertos los puertos y servicios necesarios para ejecutar eGroupWare. Más puertos abiertos significa que un atacante tiene más posibilidades de encontrar una vulnerabilidad en el servidor. Si necesita tener otros puertos abiertos, que no son necesarios para eGroupWare, entonces puede usar un cortafuegos o TCP Wrappers. Si es posible, permita servicios sólo con Secure Socket Layer (SSL) activado para el servidor eGroupWare.

6.1.1.1 Puertos que el servidor eGroupWare necesita para su ejecución

Los puertos que se necesitan son:

Puerto del servidor web:	HTTP/80
Puerto SSL del servidor web:	HTTPS/443
Administración remota, Secure Shell:	SSH/22

Si tiene que ejecutar un servidor de correo en la misma máquina, entonces necesita algunos puertos más. Si puede la oportunidad de ejecutar el servicio de correo en otra máquina, hágalo.

Email Server MTA:	SMTP/25
Email Server MTA:	SMTPS/465

Para recoger los correos del servidor con otros clientes de correo, como los clientes de correo eGroupWare, necesita uno de los siguientes puertos.

Servidor IMAP :	IMAP/143
Servidor IMAP SSL:	IMAPS/993
POP-3:	POP-3/110
POP-3 sobre SSL:	POP-3/995

Si bloquea sus puertos con un cortafuegos, por favor, tenga cuidado de que necesita algún tráfico saliente que debe permitir. Este puede ser NTP, búsquedas DNS ...

Conclusión:

El servidor necesita, al menos, los puertos: 22, 80, 443

Y como máximo, los puertos:	22, 25, 80, 110, 143, 443, 465, 993, 995
Mínimo recomendado:	22, 443
Máximo recomendado:	22, 25, 443, 993, 995

6.1.1.2 El escaneador de puertos

Para comprobar su instalación contra los puertos abiertos hay varias herramientas disponibles. Aquí mostraré sólo una, que está disponible para *NIX y Windows, y se puede encontrar en: http://www.insecure.org/nmap

Instale Nmap en su máquina y compruebe los puertos abiertos que tenga su servidor.

6.1.1.3 Salida de un escaneador de puertos

Aquí hay un ejemplo de la salida de Nmap contra un servidor. Nmap muestra los puertos que están disponibles en este servidor.

```
[root@server root]# nmap -sV servidor.com
Starting nmap 3.45 (http://www.insecure.org/nmap/ ) at 2003-09-17 00:48 CEST
Interesting ports on xxx.xxx.xx.xxx:
(The 1651 ports scanned but not shown below are in state: closed)
PORT    STATE    SERVICE    VERSION
22/tcp  open     ssh        OpenSSH 3.1p1 (protocol 2.0)
80/tcp  open     http       Apache httpd 1.3.27 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.12
    OpenSSL/0.9.6b PHP/4.1.2 mod_perl/1.26)
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
443/tcp open     ssl        OpenSSL
```

Nmap run completed -- 1 IP address (1 host up) scanned in 23.000 seconds

6.1.1.4 Desactivar servicios que no se necesitan

Si ha encontrado servicios que se ejecutan en su servidor y que no necesita, entonces deténgalos. Después de reiniciar, el servicio no volvería a iniciarse automáticamente.

En una instalación de Red Hat, se pueden usar los siguientes comandos para para un servicio y deshabilitarlo:

```
[root@server home]# service name_from_the_service stop

[root@server home]# chkconfig –level 345 name_from_the_service off
```

En uns instalación de Debian, se pueden usar las siguientes herramientas:

```
Server:~# /etc/init.d/ name_from_the_service stop
```

```
Server:~# rcconf
```

6.1.2 Desinstalar programas que no se necesitan en el servidor

En la instalación estándar, el programa de instalación instalará muchos programas que no son necesarios.
Por motivos de seguridad, borre estos programas de su servidor. Programas que no se necesitan, por ejemplo, son:
clientes ftp, wget, gcc, ficheros de cabeceras, código fuente…

Para comprobar qué paquetes están instalados en un sistema Linux basado en rpm, hay que escribir:

```
[root@server home]# for i in `rpm –qa`; do rpm –qi $i >> rpm_packages; done

[root@server home]# less rpm_packages
```

Borre todos los paquetes que no necesite

```
[root@server home]# rpm –e package
```

Para comprobar los paquetes que están instalados en un sistema Debian. Hay muchas herramientas para ello. Una es:

```
Server:~# aptitude
```

6.1.3 Comprobación local de existencia de un rootkit

Chkrootkit es una herramienta para buscar localmente signos de la existencia de un rootkit. Chkrootkit ha sido probado en: Linux 2.0.x, 2.2.x y 2.4.x, FreeBSD 2.2.x, 3.x, 4.x y 5.x, OpenBSD 2.x y 3.x., NetBSD 1.5.2, Solaris 2.5.1, 2.6 y 8.0, HP-UX 11, True64 y BSDI. Contiene:

- chkrootkit: shell script que comprueba los binarios del sistema por si los modifica el rootkit. Se realizan las siguientes pruebas:

  aliens asp bindshell lkm rexedcs sniffer wted w55808 scalper slapper z2 amd basename biff chfn chsh cron date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf init identd killall ldsopreload login ls lsof mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w write

- ifpromisc.c: comprueba si la interfaz está en modo promiscuo.
- chklastlog.c: comprueba los últimos borrados de logs.
- chkwtmp.c: comprueba borrados wtmp.
- check_wtmpx.c: comprueba borrados wtmpx. (Solaris)
- chkproc.c: comprueba signos de troyanos LKM
- chkdirs.c: comprueba signos de troyanos LKM.

- strings.c: sustitución de cadenas rápidas y sucias

Se puede descargar chkrootkit como paquete rpm compilado o como un paquete tar.gz

chkrootkit.tar.gz

chkrootkit rpm

6.1.3.1 Fragmento de ejemplo de chkrootkit

Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found

6.1.3.2 Instalar el rpm de chkrootkit

El rpm de chkrootkit debe ejecutarse en todas las distribuciones basadas en rpm.
Descárguelo de la dirección anterior e instálelo

```
[root@server tmp]# rpm –ivh chkrootkit-x.xx-x.i386.rpm
```

Después de la instalación, puede ajustar el fichero chkrootkit_cronfile a sus necesidades. Este paso no es necesario, pero hace que el informe sea menos repetitivo

```
[root@server tmp]# vi /etc/cron.daily/chkrootkit_cronfile

#!/bin/sh
cd /usr/bin ./chkrootkit 2> /dev/null | mail –s "chkrootkit output" root
```

Cambie los siguientes valores:

"chkrootkit output"	a	"chkrootkit **miservidor** output"
root	a	your_email_adress@suservidor.com

6.1.3.3 Instalar chkrootkit desde un tar.gz

Descomprima e instale chkrootkit

```
[root@server tmp]# cp chkrootkit.tar.gz /usr/local; rm chkrootkit.tar.gz
```

```
[root@server tpm]# cd /usr/local/

[root@server local]# tar xzvf chkrootkit.tar.gz

[root@server local]# mv chkrootkit-x.xx chkrootkit

[root@server local]# chown –R root.root chkrootkit
[root@server chkrootkit]# cd chkrootkit

[root@server chkrootkit]# make sense
```

Para hacer que chkrootkit le envíe el informe, tiene dos posibilidades. Crear un fichero chkrootkit_cronfile o añadir una línea al fichero crontab.

```
Cree un fichero chkrootkit_cronfile
[root@server cron.daily]# vi chkrootkit_cronfile

#!/bin/sh
cd /usr/local/chkrootkit ./chkrootkit 2> /dev/null | mail –s “chkrootkit myserver output”
your_email_adress

Añada la siguiente línea al fichero crontab
0  1    * * *   root    (cd /usr/local/chkrootkit; ./chkrootkit 2>&1 | mail –s
 "chkrootkit output" su_dirección_de_correo)

Ahora, chkrootkit le enviará un informe a la dirección de correo indicada arriba.
```

6.1.4 Administradión de un servidor seguro

Si desea administrar su servidor de forma segura, entonces use el protocolo SSH. Con este protocolo, todas las conexiones quedan cifradas. Con protocolos como telnet y ftp, las cuentas de usuario y sus contraseñas se transmiten sin cifrar (en texto claro). La transferencia de las cuentas y las contraseñas es fácil de “esnifar" para un atacante. Con las contraseñas esnifadas, un hacker puede iniciar una sesión usando esos datos.

Si es posible, use sólo conexiones SSH 2 y no SSH 1. Tampoco use su cuenta de root para iniciar la sesión en un servidor remoto. Conéctese al servidor remoto con una cuenta normal de usuario y use su o sudo para las tareas de administración en el servidor.

6.1.4.1 Conéctese a su servidor con una sesión segura

Si su servidor soporta conexiones SHH, entonces es fácil administrarlo remotamente. Sólo tiene que conectarse al servidor con su cliente SSH.

Si se conecta al servidor la primera vez, recibirá una advertencia como la siguiente. Debe responder a la advertencia con "yes", si está seguro de que éste es el servidor al que desea conectarse.

```
[user@client home]$ ssh suservidor
The authenticity of host 'yourserver (100.178.76.207)' can't be established.
RSA key fingerprint is 7e:8e:55:8b:49:57:5d:41:40:ab:93:64:18:af:60:ea.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'yourserver' (RSA) to the list of known hosts.
```

- Conéctese a su servidor para la administración remota

```
[user@client home]$ ssh suservidor
```

- Copie los ficheros a su servidor con secure copy (scp)

```
[user@client home]$ scp fichero.txt servidor:/home/
```

- También puede usar sftp para trabajar con un "cliente ftp seguro"

```
[user@client home]$ sftp servidor
```

En algunas instalacines, la función sftp está desactivada por defecto (por ejemplo por Debian). Si quiere activarla, debe añadir la siguiente línea al fichero sshd_config en su servidor.

En un sistema Debian debe ser:

```
subsystem sftp /usr/lib/sftp-server
```

En un sistema RedHat debe ser:

```
subsystem sftp /usr/libexec/openssh/sftp-server
```

6.1.4.2 Trabajando con pares de claves SSH

Trabajar con pares de claves SSH tiene sus ventajas. La primera es que no necesita escribir su contraseña cada vez que se conecte al servidor, y la segunda, es que es más seguro usar pares de claves. Cuando se usan pares de claves, se puede permitir el uso de contraseña por en el servidor para la identificación.

Para cada usuario que quiera conectarse al servidor, hace falta un par de claves

6.1.4.2.1 Crear un par de claves seguras

El par de claves debe crearse en el lado del cliente

```
[user@client home]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
```

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /user/.ssh/id_dsa.
Your public key has been saved in /user/.ssh/id_dsa.pub.
The key fingerprint is:
f0:00:f7:95:e9:73:37:11:aa:e8:06:3e:60:9e:0d:25 user@yourserver
```

6.1.4.2.2 Copiar la clave pública al servidor

Tiene que copiar su nueva clave pública (*.pub) de su máquina local al servidor.

```
[user@client home]$ scp .ssh/id_dsa.pub useratserver@yourserver:/home/yoursername/
```

Instale la clave pública en el servidor.

```
[user@client home]$ ssh servidor
[user@server home]$ cat id_dsa.pub >> .ssh/authorized_keys
[user@client home]$ chmod  600 .ssh/authoritzed_keys
```

Ahora, si se conecta al servidor, éste le pide la contraseña que escribió cuando se creó el par de claves. Si no quiere escribirlo cada vez, puede usar ssh-add

6.1.4.2.3 La herramienta ssh-add

Si se conecta al servidor (o distintos servidores) con frecuencia, puede usar la herramienta ssh-add para almacenar la contraseña desde su clave ssh. Aquí, escriba la contraseña una vez y ya se queda almacenada.

```
[user@client home]$ ssh-add
Enter passphrase for /home/youruser/.ssh/id.dsa:
Identify added: /home/youruser/.ssh/id.dsa (/home/youruser/.ssh/id.dsa)
```

6.1.4.2.4 Seguridad en su cliente SSH

En el fichero de configuración del cliente SSH hay una línea importante. El valor en el fichero ssh_config debe ser, por motivos de seguridad:

```
Protocol 2
```

Esto permite las conexiones de sus clientes sólo con la versión 2 del protocolo SSH

6.1.4.2.5 Seguridad en el servidor SSHD

En el demonio SSH puede usar los siguientes valores para hacerlo más seguro:

```
Protocol 2
PermitRootLogin no
PubKeyAuthetifikation yes
```

```
PasswordAuthentification no
PermitEmptyPassword no
```

6.1.5 Instalar software para monitorizar los registros del sistema

Analizar los ficheros de registro del sistema es una obligación para cada administrador. Si no se vigilan estos ficheros, no se pueden conocer los problemas de segurida o las anomalías. Existen varios productos en el mercado para monitorizar los ficheros de registro del sistema.

logcheck

logwatch

logsurfer

El producto que quiero recomendar aquí es logcheck. Logcheck funciona en Linux, BSD, Sun, HP-UX. Es fácil de instalar y hacer informes claros. Para instalar logcheck, escriba lo siguiente desde la raíz del código fuente después de haber descomprimido el fichero.

```
[root@server logcheck-1.1.1]# make linux
```

Para ejecutarlo automáticamente, debe añadir una línea al fichero crontab. En RedHat, es /etc/crontab. Abra el fichero y añada la siguiente línea:

```
00 * * * * root /bin/sh /usr/local/etc/logcheck.sh
```

Edite el script logcheck para añadir el destinatario para el informe del sistema. El destintario es el administrador del sistema en el script.

```
[root@egroupware logcheck-1.1.1]# vi /usr/local/etc/logcheck.sh
```

Para recibir informes más detallados, los usuarios avanzados pueden editar también los siguientes ficheros:

logcheck.violations
logcheck.violations.ignore
logcheck.hacking
logcheck.ignore

6.1.6 Entorno de detección de intrusos

Instale un entorno de detección de intrusos para comprobar la integridad de ficheros y detectar cambios en el servido.
Existen varias soluciones disponibles para sistemas basados en *nix.

AIDE

Tripwire

Samhain

De los tres IDS (Sistemas de detección de intrusos – Intruder Detection System) basados en host citados, AIDE es el más fácil de configurar.

6.1.6.1 Instalación de Aide

La mayoría de las distribuciones incluyen AIDE, por lo que se puede instalar con las herramientas habituales de las distribuciones como rpm o apt-get.
AIDE depende del paquete mhash, que también hay que instalar. Si el paquete no está disponible, entonces hay que compilarlo.

```
./configure
make
make install
```

6.1.6.2 El fichero de configuración de Aide, aide.conf

Debe configurarse el fichero the aide.conf para que todos los ficheros importantes del servidor se comprueben, y reducir así falsas alarmas.

Guarde /etc/aide.conf, /usr/sbin/aide y /var/lib/aide/aide.db.gz en una ubicación segura, por ejemplo, en soporte separado y de sólo lectura (como un CD-ROM). También guarde huellas MD5 o firmas GPG de esos ficheros en una ubicación segura, para poder comprobar de manera fiable posteriormente si los ficheros han sido modificados.

```
# Ejemplo de fichero de configuración para AIDE.
@@define DBDIR /var/lib/aide

# La ubicación de la base de datos (lectura).
database=file:/mnt/floppy/aide.db.gz

# La ubicación de la base de datos (escritura).
database_out=file:@@{DBDIR}/aide.db.new.gz

# Si se usa gzip al escribir en la base de datos
gzip_dbout=yes

# Valor predeterminado.
verbose=5

report_url=file:/var/log/aide.log
report_url=stdout

# Reglas predeterminadas.
#
#p:      permissions
#i:      inode:
#n:      number of links
#u:      user
```

```
#g:      group
#s:      size
#b:      block count
#m:      mtime
#a:      atime
#c:      ctime
#S:      check for growing size
#md5:    md5 checksum
#sha1:   sha1 checksum
#rmd160: rmd160 checksum
#tiger:  tiger checksum
#haval:  haval checksum
#gost:   gost checksum
#crc32:  crc32 checksum
#R:      p+i+n+u+g+s+m+c+md5
#L:      p+i+n+u+g
#E:      Empty group
#>:      Growing logfile p+u+g+i+n+S

# Se pueden crear reglas personalizadas, como ésta.
NORMAL = R+b+sha1
DIR = p+i+n+u+g

# A continuación, decida los ficheros y directorios que desee que estén en la base de datos.

/boot   NORMAL
/bin    NORMAL
/sbin   NORMAL
/lib    NORMAL
/opt    NORMAL
/usr    NORMAL
/root   NORMAL

# Comprobar sólo los permisos, inode, usuario y grupo para /etc, pero
# vigilando algunos ficheros importantes.
/etc    p+i+u+g
!/etc/mtab
/etc/exports  NORMAL
/etc/fstab    NORMAL
/etc/passwd   NORMAL
/etc/group    NORMAL
/etc/gshadow  NORMAL
/etc/shadow   NORMAL
```

Ejecute "aide --init" para construir la base de datos inicial.

```
[root@server root]# /mnt/floppy/aide --init
```

Copie /var/lib/aide/aide.db.new.gz a la ubicación segura

```
[root@server root]# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz
```

Compruebe las inconsistencias de su sistema comparadas con la base de datos de AIDE. Antes de ejecutar una comprobación manualmente, asegúrese de que el el binario y la base de datos AIDE no se han modificado sin su conocimiento.

```
[root@server root]# /mnt/floppy/aide --check
```

6.1.6.3 Crear un fichero cron para ejecutar Aide automáticamente

Este fichero está incluido en el paquete de Debian AIDE, así que no necesita crear este fichero si usa el paquete de Debian. El fichero, que se usa aquí como un ejemplo, es un fichero modificado de RedHat / Fedora Linux. Si desea crear un fichero cron para otra distribución, debe cambiar las rutas.

```
#!/bin/sh

PATH="/bin:/usr/sbin:/usr/bin"
LOGFILE="/var/log/aide.log"
CONFFILE="/etc/aide.conf"
ERRORLOG="/var/log/error.log"

[ -f /usr/sbin/aide ] || exit 0

MAILTO=”yourusername”
DATABASE=`grep "^database=file:/" $CONFFILE | head -1 | cut -d: -f2`
LINES=”1000”
FQDN=`hostname -f`
DATE=`date +"at %X on %x"`

[ -z "$MAILTO" ] && MAILTO="root"

if [ ! -f $DATABASE ]; then
        (
        echo "Fatal error: The AIDE database does not exist!"
        echo "This may mean you haven't created it, or it may mean that someone has removed
it."
        ) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO
        exit 0
fi
```

```
aide --check >$LOGFILE 2>$ERRORLOG

(cat << EOF;
This is an automated report generated by the Advanced Intrusion Detection
Environment on $FQDN ${DATE}.

EOF
if [ -s $LOGFILE ]; then
        loglines=`wc -l $LOGFILE | awk '{ print $1 }'`
        if [ ${loglines:=0} -gt $LINES ]; then
                echo
                echo "TRUNCATED (!) output of the daily AIDE run:"
                echo "Output is $loglines lines, truncated to $LINES."
                head -$LINES $LOGFILE
                echo "The full output can be found in $LOGFILE."
        else
                echo "Output of the daily AIDE run:"
                cat $LOGFILE
        fi
else
        echo "AIDE detected no changes."
fi
if [ -s $ERRORLOG ]; then
        errorlines=`wc -l $ERRORLOG | awk '{ print $1 }'`
        if [ ${errorlines:=0} -gt $LINES ]; then
                echo "TRUNCATED (!) output of errors produced:"
                echo "Error output is $errorlines lines, truncated to $LINES."
                head -$LINES $ERRORLOG
                echo "The full output can be found in $ERRORLOG."
        else
                echo "Errors produced:"
                cat $ERRORLOG
        fi
else
        echo "AIDE produced no errors."
fi
) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO
```

No se recomienda que se ejecuten comprobaciones automatizadas de AIDE sin comprobar por uno mismo AIDE con frecuencia.
Además, AIDE no implementa ninguna protección por contraseña o cifrado para sus propios ficheros.

6.1.6.4 Informe de ejemplo de AIDE

El informa que crea AIDE, muestra todos los cambios en el sistema de ficheros. Por favor, compare el informe con los cambios que haya hecho (instalar una actualización o cambiar la configuración desde su servidor).

This is an automated report generated by the Advanced Intrusion Detection Environment on egroupware at 05:27:16 PM on 02/14/2004.

Output of the daily AIDE run:
AIDE found differences between database and filesystem!!
Start timestamp: 2004-02-14 17:27:16
Summary:
Total number of files=34691,added files=2,removed files=0,changed files=5

Added files:
added:/etc/cron.daily/aide
added:/var/log/error.log
Changed files:
changed:/etc/aide.conf
changed:/root
changed:/root/.viminfo
changed:/root/.bash_history
changed:/root/chkrootkit-0.43-1.i386.rpm
Detailed information about changes:

File: /etc/aide.conf
Inode : 89090 , 89173

Directory: /root
Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12

File: /root/.viminfo
Size : 6683 , 6513
Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Inode : 111362 , 111363
MD5 : UM0erzXMWPEdiCgKV/t91g== , l9E0UBQu7PKTCJiS3b2Fzw==
SHA1 : jNlzWrSY/Q4zk3Rd7dnpyth2a0Y= , R1wFnTg2scWSaRnn47zcZ+syS3E=

File: /root/.bash_history
Size : 14824 , 14872
Mtime : 2004-02-14 16:16:30 , 2004-02-14 16:48:32

```
Ctime    : 2004-02-14 16:16:30                  , 2004-02-14 16:48:32
MD5      : zlVCx+39n8XLd3/ip757vA==             , nCs18yzJdwDD/BfsUssuhQ==
SHA1     : Al8brD3i+B6P2RMxpn6IaC+I5fE=         , bWBEjLA0Hnt6XXTszkzKi8gaTZQ=

File: /root/chkrootkit-0.43-1.i386.rpm
Permissions: -rw-r--r--                         , -rw-r-----
Ctime    : 2004-01-26 13:43:35                  , 2004-02-14 16:51:06

                AIDE produced no errors.
```

6.1.6.5 Crear una base de datos nueva después de los cambios

Después de comprobar el informe, debe crear una nueva base de datos y guardarla en la ubicación segura. ¡Ejecute la actualización de su base de datos después de cada informe que haya comprobado!.

```
[root@server root]# /mnt/floppy/aide --init

[root@server root]# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz
```

6.1.7 Seguridad de los servicios en demonios

Ejecute los demonios necesarios en un entorno chroot en *nix

Use TCP Wrappers o xinetd para la seguridad en los demonios

6.1.8 Cortafuegos

Configure un cortafuegos en su servidor para proteger su sistema.

6.2 Seguridad en aplicaciones web

Con un software de seguridad en aplicaciones, se puede ejecutar de forma segura sus aplicaciones basadas en web, como eGroupWare, desde ejecuciones SQL, Cross Side Scripting y otros ataques. Hay varias aplicaciones en el mercado Apache e IIS. Dos herramientas libres son:

ModSecurity (para Apache Webserver 1.3x y 2.x)
IISShield (Para Internet Information Server)

ModSecurity es una herramienta libre de detección de intrusos para aplicaciones web. Opera empotrada en el servidor web, actuando como un paraguas potente, poniendo un escudo a las aplicaciones para protegerlas de los ataques. ModSecurity soporta Apache 1.3x y Apache 2.x.

6.2.1 Instalar ModSecurity

Descomprima el código fuente de mod_security.

```
[root@server tmp]# tar xzvf mod_security-x.x.x.tar.gz
```

Vaya al directorio de mod_security

```
[root@server tmp]# cd mod_security-x.x.x/apache2
```

Puede compilar el módulo como módulo DSO (Dynamic Shared Object) o de forma estática. Si quiere hacerlo estático, debe recompilar Apache. Aquí sólo se describe el uso de ModSecurity como módulo DSO.

```
[root@server apache2]# apxs -cia mod_security.c
```

En Redhat, añada la siguiente línea a su httpd.conf en la sección donde se cargan los módulos.

```
[root@server mod_security-1.7.4]# vi /etc/httpd/conf/httpd.conf

Include /etc/httpd/conf.d/mod_security.conf
```

Debe reiniciar Apache para activar ModSecurity

```
[root@server mod_security-1.7.4]# apachectl stop
[root@server mod_security-1.7.4]# apachectl start
```

6.2.2 Configuración básica

Mod Security tiene algúna configuración de ejemplo incluida para configurarlo. También puede convertir las reglas de Snort para usarlo desde ModSecurity. Las reglas de ejemplo de Snort se pueden encontrar en el servidor del proyecto o convertiras usted mismo.

```
<IfModule mod_security.c>

  # Activar o desactivar
  SecFilterEngine On

  # Asegurarse de que el juego de caracteres es válido
  SecFilterCheckURLEncoding On

  # El motor de auditoría funciona de manera independiente y
  # se puede activar o desacativar por servidor o
  # por-directorio. "On" grabará todo en el registro del sistema,
  # "DynamicOrRelevant" grabará las solicitudes o violaciones dinámicas,
  # y "RelevantOnly" grabará sólo las violaciones de políticas
  SecAuditEngine RelevantOnly

  # El nombre del fichero de registro de auditoría
  SecAuditLog logs/audit_log

  SecFilterDebugLog logs/modsec_debug_log
  SecFilterDebugLevel 0

  # ¿Inspeccionar POST payloads?
  SecFilterScanPOST On
```

```
# Acción predeterminada
SecFilterDefaultAction "deny,log,status:500"

# Prevenir ataques de rutas (..)
SecFilter "\.\./"

# Protección débil XSS, pero permite etiquetas HTML comunes
SecFilter "<[[:space:]]*script"


# Filtros para prevenir ataques de comandos SQL
SecFilter "delete[[:space:]]+from"
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"

# Requerir cabeceras HTTP_USER_AGENT y HTTP_HOST
SecFilterSelective "HTTP_USER_AGENT|HTTP_HOST" "^$"

</IfModule>
```

Tenga cuidado. La configuración de ModSecurity depende de los módulos que use. Debe hacer ajustes muy específicos al recibir errores. Use sólo losfiltros necesarios para su servidor. Si usa un servidor Linux, no necesita comprobar las reglas de Windows.

6.2.3 Comprobar ModSecurity

Puede hacer una prueba rápida de la funcionalidad de ModSecurity. Vaya al directorio test en modsecurity y ejecute alguna de las pruebas de ejemplo.

```
[root@server tests]# ./run-test.pl yourIpAdress 09-directory-traversal-in-parameters.test
11-xss-attack.test 13-sql-injection.test

Test "09 Directory traversal in parameters": Failed (status = 406)
Test "11 XSS attack": Failed (status = 406)
Test "13 SQL injection": Failed (status = 406)
```

6.2.4 Registro de ejemplo de ModSecurity

Aquí verá un registro de ejemplo de las pruebas anteriores.

```
Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0" 406 352
Handler: cgi-script
---------------------------------------
GET /cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0
```

Host: xxx.xxx.xxx.xxx :80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match "\.\./"
at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
==========

Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0" 406
352
Handler: cgi-script

GET /cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0
Host: xxx.xxx.xxx.xxx:80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match "<(
|\n)*script" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
==========
Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0" 406 352
Handler: cgi-script

GET /cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0
Host: xxx.xxx.xxx.xxx
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406. Pattern match
"delete[[:space:]]+from" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable

```
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

6.3 Optimización y seguridad en Apache

Para la seguridad del servidor web, debe desactivar todos los módulos innecesarios. Active sólo lo que necesite para ejecutar el servidor web. Ejecutarlo con menos módulos, también mejora el rendimiento.

6.3.1 Módulos recomendados

Los siguiente módulos dan una breve descripción de lo que se necesita para ejecutar Apache 2 con eGroupWare. Los demás módulos debe desactivarse.

¡La optimización de Apache no es para gente inexperta! Si desactiva alguos módulos en httpd.conf, también debe comentar otras opciones en httpd.conf. Se recomienda desactivar un módulo, para el servidor y reiniciarlo. Eche un vistazo a los mensajes de error.

```
mod_access.so
mod_auth.so
mod_include.so
mod_log_config.so
mod_expires.so
mod_deflate.so
mod_headers.so
mod_unique_id.so
mod_setenvif.so
mod_mime.so
mod_negotiation.so
mod_dir.so
mod_alias.so
```

6.3.2 Otras opciones de configuración de Apache

Se puede esconder mucha información de Apache por motivos de seguridad. Hay distintas posibilidades para Apache 1.3 y Apache 2.x.

La directiva ServerTokens en httpd.conf debe contener el valor OS, ExtendedStatus debe estar en Off. ServerSignature, OFF, el directorio del manual /var/www/manual en Deny from all. Si no necesita cgi-bin, desactívelo. En AddHandler, type-map INCLUDES, comentar con #. En /var/www/error poner Order deny,allow en Deny from all. Los ficheros /server-status y /server-info no deben ser de lectura pública por motivos de seguridad.

6.4 Turck MMCache

Turck MMCache es un acelerador PHP de código abierto, que optimiza, codifica y tiene un caché de contenidos dinámico. Incrementa el rendimiento de scripts PHP cacheándolos en estado compilado,así que la sobrecarga de compilar de elimina casi completamente. También usa algunas optimizaciones para ejecutar más rápidamente los scripts PHP. Turck MMCache suele reducir la carga en el servidor e incrementa la velocidad del código PHP de 1-a 10 veces.

Para más información sobre TurckMMCache visite la página de desarrollo.

6.4.1 Requisitos

Se necesita phpize para crear el script configure. Compruebe que esté disponible desde phpize con search o locate. En Fedora Linux, debe instalar php-devel para compilar mmcache.

RedHat Enterprise Linux 3 se suministra sin el paquete phpize. Tiene que compilar de nuevo el paquete PHP y crear dos paquetes de desarrollo.

6.4.1.1 Tareas previas en RedHat Enterprise Linux 3

Para crear los paquetes de desarrollo PHP, necesia los siguientes paqutes:

bzip2-devel curl-devel db4-devel expat-devel freetype-devel gd-devel gdbm-devel gmp-devel pspell-devel httpd-devel libjpeg-devel, libpng-devel pam-devel libstdc++-devel libxml2-devel ncurses-devel openssl-devel zlib-devel pcre-devel imap-devel

Los paqutes pcre-devel e imap-devel no se ofrecen desde RedHat, así que tiene que compilarlos usted mismo. Descargue los srpm en su servidor y cópielos en /usr/src/redhat/SRPMS para crear los paquetes de desarrollo.

```
[root@server SRPM]#rpmbuild –rebuild pcre-x.x-xx.src.rpm
[root@server SRPM]#rpmbuild –rebuild imap-x.x-xx.src.rpm
```

Vaya al directorio RPM e instale los rpms de desarrollo necesarios en su servidor

```
[root@server SRPM]#cd /usr/src/redhat/RPM/i386
[root@server i386]#rpm –ivh pcre-devel-x.x-xx.i386 imap-devel-xxxxx-x.rpm
```

Instale el rpm fuente de PHP en su servidor y vaya al directorio SPEC

```
[root@server SRPM]#cd /usr/src/redhat/SPEC
```

Ahora, hay que editar el fichero php.spec con vi o vim

Después de la línea 55, añada las siguientes líneas al fichero:

```
%package devel
Group: Development/Libraries
Summary: Files needed for building PHP extensions.


%description devel
The php-devel package contains the files needed for building PHP
extensions. If you need to compile your own PHP extensions, you will
need to install this package.
```

Cambiar la siguiente línea:

```
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize,php-config,phpextdist,phpize}
Y poner en su lugar:
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize}
```

Borrar esta línea:

```
rm -rf $RPM_BUILD_ROOT%{_includedir} \
$RPM_BUILD_ROOT%{_libdir}/php
```

Añadir este bloque después de la primero sección %files

```
%files devel
%defattr(-,root,root)
%{_bindir}/php-config
%{_bindir}/phpize
%{_bindir}/phpextdist
%{_includedir}/php
%{_libdir}/php
```

Guarde el fichero y compile el nuevo paquete

```
[root@server SPECS]# rpmbuild –bb php.spec
```

¡Instale SOLO el paquete php de desarrollo en su servidor!

6.4.2 Compatibilidad

Esta versión de Turck MMCache ha sido comprobado correctamente en PHP 4.1.0-4.3.2 bajo RedHat Linux 7.0, 7.3, 8.0 RedHat ES y AS y Windows con Apache 1.3 y 2.0.

6.4.3 Instalación rápida

- compilar Turck MMCache

  export PHP_PREFIX="/usr"
  $PHP_PREFIX/bin/phpize
  ./configure –enable-mmcache=shared –with-php-config=
  $PHP_PREFIX/bin/php-config
  make

  Debe especificar el prefijo real donde esté instalado PHP con el comando "export". Puede ser "/usr" "/usr/local" o cualquier otra cosa.

- Instalar Turck MMCache

  make install

- Configurar Turck MMCache

  Turck MMCache puede instalarse como una extensión Zend o PHP. Es necesario editar el fichero your php.ini, que suele estar en /etc/php.ini

  Para instalar como una extensión Zend:

  zend_extension="/usr/lib/php4/mmcache.so"
  mmcache.shm_size="16"
  mmcache.cache_dir="/tmp/mmcache"

mmcache.enable="1"
mmcache.optimizer="1"
mmcache.check_mtime="1"
mmcache.debug="0"
mmcache.filter=""
mmcache.shm_max="0"
mmcache_ttl="0"
mmcache.shm_prune_period="0"
mmcache.shm_only="0"
mmcache.compress="1"

Si usa una compilación "thread safe" de PHP, debe usar "zend_extensions_ts" en lugar de "zend_extension"

Para instalar como extensión PHP:

extension="mmcache.so"
mmcache.shm_size="16"
mmcache.cache_dir="/tmp/mmcache"
mmcache.enable="1"
mmcache.optimizer="1"
mmcache.check_mtime="1"
mmcache.debug="0"
mmcache.filter=""
mmcache.shm_max="0"
mmcache_ttl="0"
mmcache.shm_prune_period="0"
mmcache.shm_only="0"
mmcache.compress="1"
mmcache.content

- Crear el directorio caché

mkdir /tmp(mmcache
chmod 0777 /tmp/mmcache

6.4.4 Interfaz web

Turck MMCache puede gestionarse mediante el script de interfaz web mmcache.php. Por lo tanto, necesita poner este fichero en su sitio web. Por razones de seguridad, se recomienda restringir el uso de esta script a su IP local.
Desde la versión 2.3.18, se puede proteger la interfaz administrativa con una contraseña. Para generar una contraseña, ejecute mmcache_password.php desde la línea de comando y siga las instrucciones.

- Crear la contraseña mmcache

[root@server turck-mmcache***]# php –q mmcache_password.php
Changing password for Turck MMCache Web Interface (mmcache.php)
Enter admin name: cacheadminname
New admin password: yourpassword

Retype new admin password: yourpassword

Add the following lines into your php.ini and restart HTTPD

mmcache.admin.name="cacheadminname"
mmcache.admin.password="$1$0ScD9gkb$nOEmFerNMvQ576hELeLrG0"

6.5 Seguridad de la instalación PHP

Ponga seguridad en sus directorios del servidor web, de tal forma que estén visibles sólo para el propio servidor web.

```
;;;;;;;;;;;;;;;;;;;
; Language Options ;
;;;;;;;;;;;;;;;;;;;

; open_basedir, if set, limits all file operations to the defined directory
; and below.  This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
open_basedir = /var/www/html:/var/www/files:/tmp:/usr/share/pear:/usr/bin/crontab

; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
expose_php = Off

;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;
max_execution_time = 30     ; Maximum execution time of each script, inseconds
memory_limit = 24M      ; Maximum amount of memory a script may consume (8MB)

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; Print out errors (as a part of the output).  For production web sites,
; you're strongly encouraged to turn this feature off, and use error logging
; instead (see below).  Keeping display_errors enabled on a production web site
; may reveal security information to end users, such as file paths on your Web
; server, your database schema or other information.
display_errors = Off
```

```
; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed.  It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off

; Log errors into a log file (server-specific log, stderr, or erro_ log (below))
; As stated above, you're strongly advised to use error logging in place of
; error displaying on production web sites.
log_errors = On

; Store the last error/warning message in $php_errormsg (boolean).
track_errors = Off

; Log errors to syslog (Event Log on NT, not valid in Windows 95).
error_log = syslog

;;;;;;;;;;;;;;;;;;;
; Data Handling ;
;;;;;;;;;;;;;;;;;;;

register_globals = OFF
```

Es más seguro poner las rutas para session.save_path y upload_tmp_dir en el fichero php.ini e incluirlas a las restricciones open basedir

6.6 Crear un certificado para el servidor web

Para proteger su privacidad, si se conecta a su instalación eGroupWare, puede usar un certificado en el servidor.
Con un certificado, se puede conectar al servidor web con una conexión cifrada (https en vez de http). Sin una conexión https, otras personas pueden usar un "sniffer" para averiguar su contraseña, u otra información.

Tiene unas pocas posibilidades para crear un certificado para el servidor web:

1.) Cree su propio autoridad de certificado y firme su certificado de servidor.
(Confianza baja)
2.) Use una Autoridad de certificación sin ánimo de lucro
https://www.cacert.org
(Confianza alta)
3.) use una Autoridad de certificado comercial
http://www.thawte.com
https://www.verisign.com

(Confianza alta)

Si quiere usar una Autoridad comercial, por favor, vaya directamente al punto 5.3.2

6.6.1 Unirse a una Autoridad de certificación (CA)

El primer paso para recibir un certificado de servidor es unirse a cacert.

Abra el navegador y vaya a la siguiente dirección: https://www.cacert.org
Siga el enlace y elija "Join CAcert" en el lado izquierdo
Continúe con la inscripción
Rellene toda la información necesaria para crear una cuenta personal en CA Cert
Después de indicar la contraseña, recibirá más instrucciones por correo electrónico.

6.6.2 Crear una solicitud de firma de certificado

En la instalación del servidor, hay que crear una clave de servidor y una solicitud de firma de certificado.

6.6.2.1 Cambiar el fichero openssl.cnf

Necesitará sólo los cambios en el fichero openssl.cnf si quiere usar el certificado de la CA sin ánimo de lucro. En Debian Linux, el fichero está en /usr/lib/ssl/, y en Red Hat la ruta es /usr/share/ssl/

Por favor, compruebe que su fichero openssl.cnf es similar al de la muestra siguiente. Las líneas importantes son las que están descomentadas o el cambio del valor stateOrProvinceName.

```
[root@server ssl]# vi openssl.cnf

# For the CA policy
[ policy_match ]
countryName                     = match
stateOrProvinceName             = optional
organizationName                = match
organizationalUnitName          = optional
commonName                      = supplied
emailAddress                    = optional


[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = GB
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = State or Province Name (full name)
```

```
#stateOrProvinceName_default            = Berkshire

localityName                            = Locality Name (eg, city)
#localityName_default                   = Newbury

0.organizationName          = Organization Name (eg, company)
#0.organizationName_default             = My Company Ltd

organizationalUnitName                  = Organizational Unit Name (eg, section)
#organizationalUnitName_default =
```

6.6.2.2 Crear la clave de servidor y solicitud de firma

Para obtener un certificado, hay que crear una clave en el servidor y una solicitud de firma para el certificado del servidor.

1.) Cree una clave para el servidor. En Debian, se almacena en /etc/ssl/certs/, y en Red Hat, en /etc/httpd/conf/ssl.csr/

El siguiente comando crea una clave de servidor protegida con contraseña. Si no tiene acceso de consola, NO cree una clave protegida mediante una contraseña, ya que el servidor esperará que se le introduzca la contraseña al iniciarse y no continuará hasta que ésta se introduzca. Si tiene acceso de consola, use la clave protegida con una contraseña, ya que es más seguro.

```
[root@server ssl]# /usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Para crear una clave que no esté protegida con una contraseña:

```
[root@server ssl]# /usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Modifique los permisos de acceso para la clave

```
[root@server ssl]# chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

2.) Ahora hay que crear la solicitud de firma del certificado. Por favor, recuerde modificar las rutas para que coincidan con las de su servidor

```
[root@server ssl]# /usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
```

-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:

El sistema le pide la contraseña, la que se le dió al crearla. Si creó la clave sin contraseña, entonces no se necesita.

You are about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:**DE**
State or Province Name (full name) []:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:**egroupware.org**
Organizational Unit Name (eg, section) []:
Common Name (your name or server's hostname) []:**egroupware.org**
Email Address []:yourname@yourdomain.org
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

In your folders, you will find a new file named server.csr. This file has to be sent to your certificate authority.

6.6.2.3 Enviar la solicitud de firma a la CA

Hay que enviar la solicitud de firma a la autoricad de certificación (CA). Aquí, lo enviamos a CA Cert.

Abra el navegador y vaya a https://www.cacert.org
Pulse en el enlace Server Certificate -> Login
Añada un dominio nuevo, Después, confirme el correo que le llegue. A continuación, siga el enlace Certificates -> Requests; copie el contenido completo del fichero server.csr en el campo de texto, y confirme que está de acuerdo con el proceso.

6.6.2.4 Instalar el certificado en el servidor

Después de enviar su fichero csr, recibirá un correo de la CA con su certificado firmado. Tiene que copiar el cuerpo completo del correo a un fichero llamado server.crt en su servidor.

Después de guardar el fichero, necesitar reiniciar el servidor web.

6.7 El servidor web

Asegure los directorios de su servidor web para que sólo pueda verlos el usuario del servidor web.

```
[root@server html]# chown -R root.webserveruser egroupware

[root@server html]# find egroupware -type d -exec chmod 550 {} \;

[root@server html]# find egroupware -type f -exec chmod 440 {} \;
```

Recomendamos asegurar el directorio de apache. Por favor, añada las siguientes líneas a su fichero httpd.conf.

```
<Directory /var/www/html/egroupware>
        <Files ~ "\.inc\.php$ | \.tpl$">
                Order allow,deny
                Deny from all
        </Files>
</Directory>
```

6.8 El servidor de bases de datos SQL

MySQL

- Asegúrese de que su base de datos está ejecutándose y que se inicia con el arranque del sistema

- Si es la primera vez que configura la base de datos MySQL, por favor, no olvide poner una contraseña al administrador de la base de datos MySQL. La contraseña en una instalación estándar está en blanco.

  Para poner una contraseña a MySQL, use el siguiente comando

  ```
  [root@server html]# mysqladmin –u root password 'new-password'
  ```

- El servidor MySQL incluye una base de datos llamada test. Esta base de datos no es necesaria en entornos en producción, por lo que le recomendamos que la borre.

  ```
  [root@server html]# mysql –u root –p
  Enter Password:
  mysql>drop database test;
  Query OK, 0 rows affected (0,03 sec)
  ```

- Añada la siguiente línea para asegurarse de que el servidor MySQL puede usarse sólamente desde la máquina localhost. Modifique el fichero /etc/my.cnf y añada la siguiente línea:

  ```
  [mysqld]
  bind-address=127.0.0.1
  ```

7 Instalación de eGroupWare

7.1 Crear la base de datos

Con la nueva versión de eGroupWare, la instalación puede crear la base de datos automáticamente. De momento, esto funciona solo con las bases de datos MySQL y PostgreSQL. Para MSSQL, debe crear la base de datos manualmente. Si quiere que eGroupWare cree la base de datos automáticamente, vaya al punto 5.3

MySQL

- Cree la base de datos y un usuario que pueda conectarse a ella

Crear la base de datos

```
[root@server html]# mysqladmin –u yourmysqladmin –p create database
Enter password:
```

Cree el usuario y darle permisos sobre la base de datos

```
[root@server html]# mysql –u yourmysqladmin –p
Enter password:
mysql> grant all on egroupware.* to egroupwaredbuser@localhost
identified by “password”
```

PostgreSQL

- Compruebe que puede conectarse a la base de datos

Desde la cuenta de root cambie a la cuenta postgres

```
[root@server html]# su - postgres
```

Edite el fichero postgresql.conf

```
-bash-2.05b$ cd data
-bash-2.05b$ vi postgresql.conf
```

El fichero debe parecerse al ejemplo de debajo

```
#Connection Parameter
tcpip_socket = true
#ssl = false
#max_connections = 32
port = 5432
```

Edite el fichero pg_hba.conf para que se parezca a este ejemplo:

```
# TYPE DATABASE USER IP_ADDRESS MASK AUTH_TYPE AUTH_ARGUMENT
local egroupware trust
host egroupwaredbname all 127.0.0.1 255.255.255.255 md5
```

El valor User está disponible a partitr de PostgreSQL 7.3.X

Reinicie el servicio de PostgreSQL y compruebe la conectividad

```
[root@server html]# /etc/init.d/postgresql restart
[root@server html]# su - postgres
bash-2.05b$ psql -h localhost template1
```

Cerra la conectividad con la base de datos

```
template1=# \q
```

- Configure la base de datos PostgreSQL

Cree un usuario que tenga derecho de acceso a la base de datos deGroupWare

```
bash-2.05b$ createuser yourdbusername –P
```

Answer the next questions with yes:

bash-2.0.5b$ Shall the new user be allowed to create databases? (y/n) Y

bash-2.0.5b$ Shall the new user be allowed to create more new users? (y/n) N

Create the new eGroupWare database

```
bash-2.05b$ createdb -U yourdbusername yourdatabasename
```

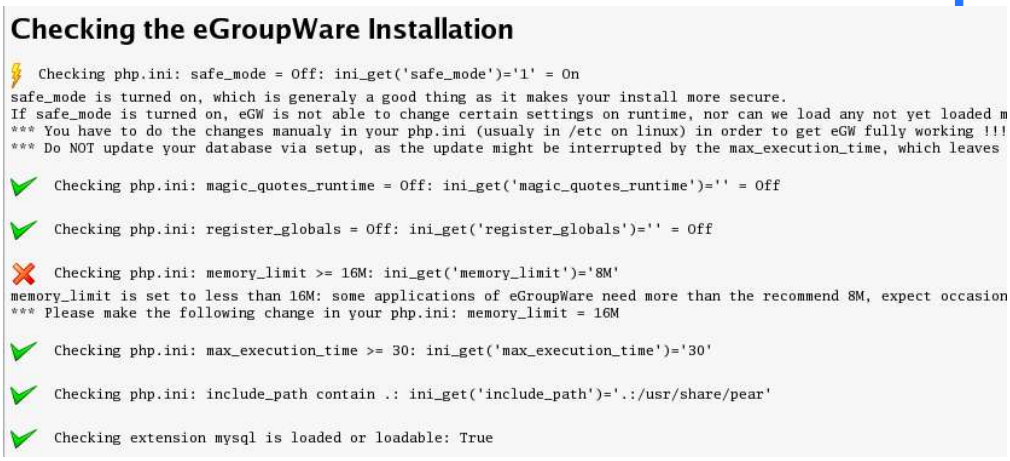
7.2 ¿Cómo iniciar la configuración?

Ponga en el navegador la URL de us instalación de egwroupware para abrir el menú de configuración.
https://www.servidor.com/egroupware/setup
Automáticamente será redirigido a la comprobación de la instalaciónde eGroupWare, que es nuestro siguiente paso.

7.3 Comprobar la instalación de eGroupWare

Si no hay un fichero header.inc.php creado, eGroupWare ejecuta una comprobación sobre algunos parámetros en el fichero php.ini y en el sistema local, y luego muestra los errores y advertencias en la configuración.

Los errores que se muestran con una cruz roja son los que tiene que resolver usted.
Las advertencias pueden ignorarse. Por ejemplo, una adevertencia en la comprobación de safe_mode. Si sabe cómo configurar las restricciones del modo seguro, esto no será problema para usted, pero para los nuevos usuarios suele ser mejor desactivar esta función.


Checking the eGroupWare Installation
Checking php.ini: safe_mode = Off: ini_get('safe_mode')='1' = On
safe_mode is turned on, which is generaly a good thing as it makes your install more secure.
If safe_mode is turned on, eGW is not able to change certain settings on runtime, nor can we load any not yet loaded m
*** You have to do the changes manualy in your php.ini (usualy in /etc on linux) in order to get eGW fully working !!!
*** Do NOT update your database via setup, as the update might be interrupted by the max_execution_time, which leaves
Checking php.ini: magic_quotes_runtime = Off: ini_get('magic_quotes_runtime')='' = Off
Checking php.ini: register_globals = Off: ini_get('register_globals')='' = Off
Checking php.ini: memory_limit >= 16M: ini_get('memory_limit')='8M'
memory_limit is set to less than 16M: some applications of eGroupWare need more than the recommend 8M, expect occasion
*** Please make the following change in your php.ini: memory_limit = 16M
Checking php.ini: max_execution_time >= 30: ini_get('max_execution_time')='30'
Checking php.ini: include_path contain .: ini_get('include_path')='.:/usr/share/pear'
Checking extension mysql is loaded or loadable: True

7.4 Crear el fichero header.inc.php

La mayoría de las partes en la configuración del fichero header.inc.php se explican por si solas.. Este menú está disponible en otros idiomas además del inglés, pero aun no se puede traducir al idioma propio (N. Del T.: esto era asi en el momento de escribir el texto, pero ya se encuentra traducido).

De momento, eGW soporta las bases de datos MySQL, PostgreSQL y MSSQL.

Con el cuadro de selección de dominio, se puede configurar más de una instalación de eGroupWare. Por ejemplo, se puede tener una instalación para cuatro empleados y otra separada para un entorno de entrenamiento.

Si configuró la base de datos manualmente, como el en paso 6.1, ha configurado un nombre, un usuario y una contraseña para la base de datos. Si quiere que el programa de configuración de eGroupWare cree la base de datos automáticamente, debe indicar esos valores aquí.

Los siguientes campos describen la base de datos y el usuario que quiere usar para conectarse a la base de datos de eGroupWare. ¡No use el usuario administrador de la base de datos para conectarse, sino que cree uno nuevo!

Servidor de la base de datos	Si la base de datos está en la misma máquina, que la instalación de eGroupWare, será localhost. También se puede elegir otro servidor para alojar la base de datos.
Nombre de la base de datos	El nombre de la base de datos que se quiere crear.
Usuario de la base de datos	El usuario que eGroupWare usa para conectarse a la base de datos.
Contraseña de la base de datos	Esta contraseña se necesita para conectarse a la base de datos
Tipo de base de datos	Seleccione el tipo de base de datos

Descargue el fichero header.inc.php creado a su máquina, y luego cópielo a la raíz de egroupware y cambie los permisos para que sólo el servidor web tenga permiso de lectura sobre este fichero.

```
[user@server tmp]$ scp header.inc.php youregwserver:/tmp
[user@server tmp]$ ssh youregwserver
[user@youregwserver user]$ su –
Password:
[root@server root]# mv /tmp/header.inc.php /var/www/html/egroupware; chmod 400
                     /var/www/html/egroupware/header.in.php;
                     chown apache /var/www/html/egroupware/header.in.php
```

Continúe en el navegador para ir al siguiente paso

7.5 Administrador de instalación/configuración

Después de la creación del fichero header.inc.php, verá una nueva ventana que le permite iniciar una sesión. Entre en el administrador de instalación/configuracón con el usuario y contraseña proporcionados en el paso anterior (7.4)

7.5.1 Paso 1 Gestión simple de aplicaciones

Aquí existen dos posibilidades: si quiere crear la base de datos automáticamente en este paso, entonces vaya ahora al punto de crear la base de datos. Si ya ha creado la base de datos, entonces vaya al punto donde se crean las tablas.

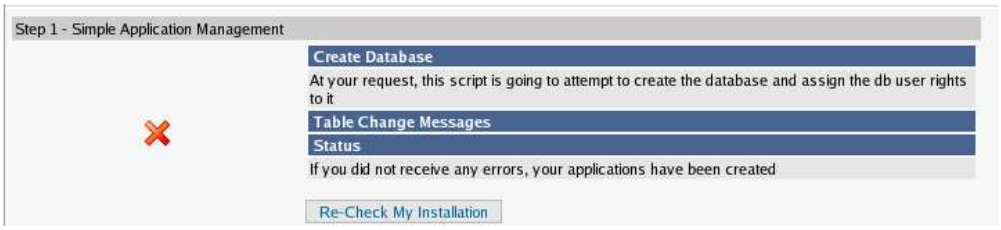
Crear la base de datos

Step 1 - Simple Application Management
Your Database is not working!
Make sure that your database is created and the account permissions are set.
Instructions for creating the database in MySql:
Login to mysql -
[user@server user]# mysql -u root -p
Create the empty database and grant user permissions -
mysql> create database egroupware;
mysql> grant all on egroupware.* to egroupware@localhost identified by 'reiner';
Or we can attempt to create the database for you:
DB root username: root
DB root password:
Create Database
Re-Check my database

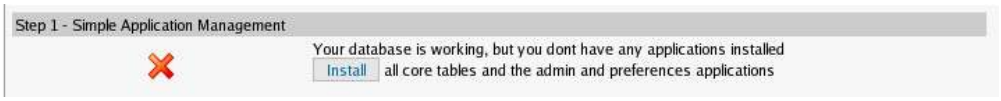
Rellene el siguiente formulario para crear la base de datos automáticamente:

Usuario root de la base de datos usuario_root
Contraseña de la base de datos contraseña de la base de datos

Y envíelo con el botón "Crear base de datos"


Step 1 - Simple Application Management
Create Database
At your request, this script is going to attempt to create the database and assign the db user rights to it
Table Change Messages
Status
If you did not receive any errors, your applications have been created
Re-Check My Installation

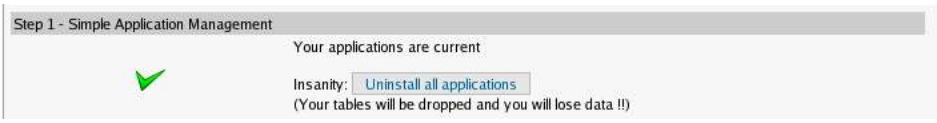
Pulse en Volver a comprobar mi instalación


Step 1 - Simple Application Management
Your database is working, but you dont have any applications installed
Install
all core tables and the admin and preferences applications

Si no ve errores, puede instalar las tablas. Pulse el botón Instalar

Step 1 - Simple Application Management
Creating Tables
At your request, this script is going to attempt to install the core tables and the admin and preferences applications for you..
Table Change Messages
Status
If you did not receive any errors, your applications have been installed
Re-Check My Installation

Ahora, mire al estado. Si no ve errorres aquí, continúe con Volver a comprobar mi instalación:


Step 1 - Simple Application Management
Your applications are current
Insanity:
Uninstall all applications
(Your tables will be dropped and you will lose data !!)

7.5.2 Paso 2 - Configuración

La mayoria de las partes en este paso se explican por sí mismas. Sólo vamos a proporcionar información que a veces puede ser confusa.

7.5.2.1 Crear el directorio para los ficheros

Hay que crear manualmente el directorio para los ficheros desde la consola del sistema. En este directorio, eGroupWare almacenará los adjuntos de las aplicaciones Registro y administrador de archivos, entre otras

¡Este directorio debe estar fuera de la ruta del servidor web! Si no sabe cuál es el directorio raíz, puede mirarlo en el fichero httpd.conf o escribir el siguientes comando (en Linux):

```
[root@server www]$ cat /etc/httpd/conf/httpd.conf | grep ^DocumentRoot
DocumentRoot "/var/www/html"
```

Cree el directorio para los ficheros y los subdirectorios necesarios.

```
[root@server www]$ mkdir /var/www/files
[root@server www]$ mkdir /var/www/files/users /var/www/files/groups
```

Tiene que dar al servidor web los permisos para leer y escribir en estos directorios.

```
[root@server www]$ chown –R apache.apache /var/www/files
[root@server www]$ chmod –R 0700 /var/www/files
```

7.5.2.2 Editar la configuración actual

Información de la ruta

Introduzca los valores necesarios para la información de sus rutas

- El directorio tmp se necesita para almacenar sesiones y otra información de la instalación de eGroupWare. Si su instalación de eGroupWare se ejecuta en una jaula chroot o con restricciones open_basedir en el fichero php.ini, cambie la ruta a los valores necesarios.

- La ruta completa para los ficheros de usuarios y grupos debe estar fuera de la raíz del servidor web por motivos de seguridad. No es posible tener este directorio dentro del ámbito del servidor web!

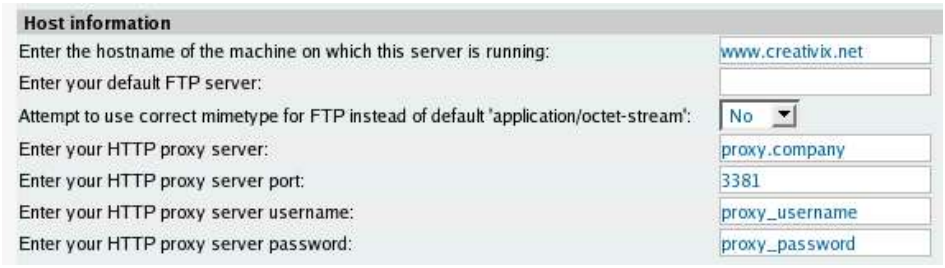
- Introduzca la URL de acceso a eGW. Si quiere usar HTTPS y HTTP, use /egroupware (sI quiere usar solo HTTPS entonces use https://servidor/egroupware)

- Por favor, no cambie el selector estándar de tipos de imágenes de su configuración predeterminada (que puede ser distinta a la del ejemplo de debajo), ya que puede romper el diseño de la interfaz gráfica

Información del servidor

- Introduzca el nombre del servidor donde esté la aplicación. Debe ser un nombre válido DNS o una dirección IP en la que se ejecuta la instalación.

- Si la instalación de eGroupWare está detrás de un servidor proxy (por ejemplo, SQUID) y quiere usar aplicaciones como cabeceras o cotizaciones, debe configurar los valores del proxy.


Host information
Enter the hostname of the machine on which this server is running:
www.creativix.net
Enter your default FTP server:
Attempt to use correct mimetype for FTP instead of default 'application/octet-stream':
No
Enter your HTTP proxy server:
proxy.company
Enter your HTTP proxy server port:
3381
Enter your HTTP proxy server username:
proxy_username
Enter your HTTP proxy server password:
proxy_password

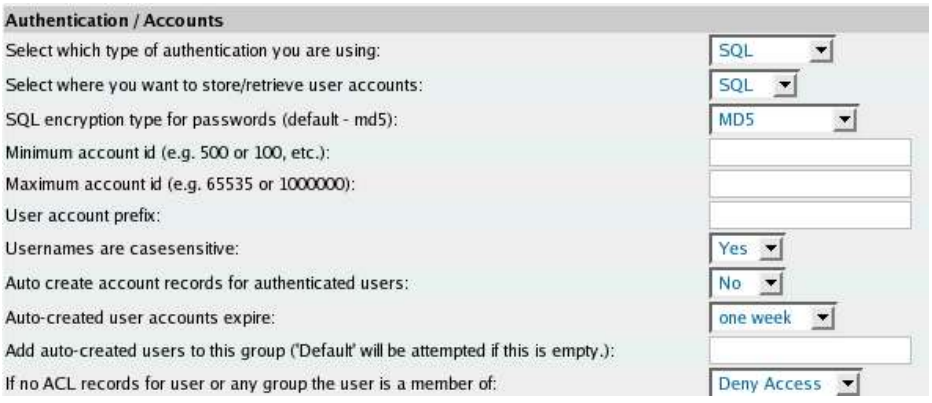
Identificación/Cuentas

- Hay disponibles varios métodos de identifación: SQL, SQL/SSL, LDAP, Mail; HTTP, NIS y Pam. Seleccione el método de identifación deseado para los usuarios de su instalación de eGroupware.

- Seleccione el tipo de cifrado para las contraseñas de los usuarios, que se almacenaran cifradas en la base de datos.

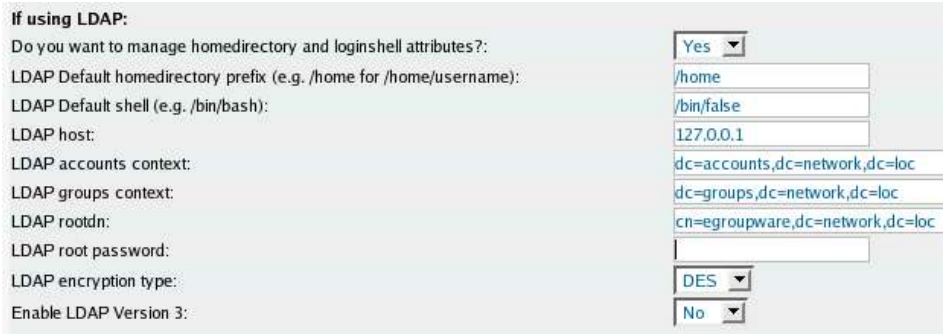
- Si quiere usar un árbol LDAP para la identificación de distintas instalaciones de eGroupWare, puede usar el prefijo de la cuenta.

- Use nombres de usuario con mayúsculas y minúsculas para mayor seguridad


Authentication / Accounts
Select which type of authentication you are using:
SQL
Select where you want to store/retrieve user accounts:
SQL
SQL encryption type for passwords (default - md5):
MD5
Minimum account id (e.g. 500 or 100, etc.):
Maximum account id (e.g. 65535 or 1000000):
User account prefix:
Usernames are casesensitive:
Yes
Auto create account records for authenticated users:
No
Auto-created user accounts expire:
one week
Add auto-created users to this group ('Default' will be attempted if this is empty.):
If no ACL records for user or any group the user is a member of:
Deny Access

Si está usandoLDAP

Si no quiere usar LDAP, no es necesario rellenar estos campos. Si quiere usar LDAP, por fovor, lea los instrucciones del fichero phpgwapi/doc/ldap/README



Configuración de Mcrypt (requiere la extensión crypt de PHP)

No todas las distribuciones tienen un mcrypt funcional compilado por defecto, así que necesita marcar esta opcion. También puede ser necesario probar varias versiones para ver cuál funciona mejor con eGroupWare.

Configuracion adicional

Los valores estándar aquí suelen funcionar correctamente.

Cuando haya terminado, guarde la configuracion.

7.5.3 Paso 3 – Configurar las cuentas de los usuarios

Aquí se crea la cuenta de administrador de eGroupWare. No use un nombre de usuario como admin, administrator, root, etc. para la contraseña del administrador, sino que mejor use letras números y caracteres especiales.
¡No cree cuentas de demostracion en entornos en produccion!

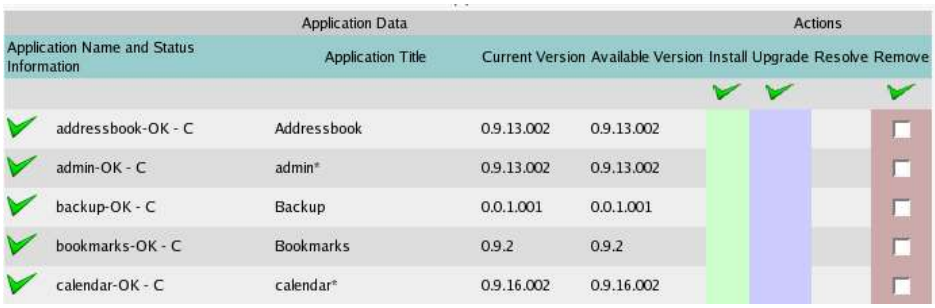
7.5.4 Paso 4 – Administrar idiomas

El idioma estándar que se instala es el inglés, asi como el idioma predeterminado en el navegador. Se pueden instalar más idiomas.

a. Puede convertir el juego de caracter automáticamente. Por ejemplo, de iso-8859-1 a UTF-8.

7.5.5 Paso 5 – Administrar aplicaciones

En la instalacion estándar, se instalan todas las aplicaciones. Para desinstalar cualquier aplicación, seleccione la casilla con el raton y pulse Guardar. Si recibe un mensaje de error acerca de dependencias, debe instalar otra aplicación. Por ejemplo, felamimail necesita que esté instalado emailadmin.



Application Data				Actions			
Application Name and Status Information	Application Title	Current Version	Available Version	Install	Upgrade	Resolve	Remove
addressbook-OK - C	Addressbook	0.9.13.002	0.9.13.002				☐
admin-OK - C	admin*	0.9.13.002	0.9.13.002				☐
backup-OK - C	Backup	0.0.1.001	0.0.1.001				☐
bookmarks-OK - C	Bookmarks	0.9.2	0.9.2				☐
calendar-OK - C	calendar*	0.9.16.002	0.9.16.002				☐

8 Iniciar una sesion en eGroupWare

Una vez que ha terminado de configurar eGroupWare, puede iniciar la sesion. Vaya a http://servidor/egroupware (o donde lo haya configurado).

El primer paso como administrador es ir a la administracion, donde se elige la configuración del sitio, los usuarios, grupos, correo electrónico y otra información necesaria.

9 Resolución de problemas

9.1 Olvido de la contraseña de administrador

¡Olvidé mi contraseña de administrador y no puedo iniciar la sesión con mi usuario de administrador en eGroupWare!

Vaya a http://servidor/egroupware/setup
Log in to Setup/Config Admin Login
Set up a new admin account.

9.2 El usuario administrador u otro usuario está bloqueado

No puedo iniciar una sesión en mi instalación de eGroupWare. Recibo el mensaje "Bloqueado, demasiados intentos". ¿Qué puedo hacer?

En la configuracion estándar, espere 30 minutos para poder volver a iniciar la sesión. Es una característica de seguridad, ¡no la desactive!

9.3 Database error: lock(Array, write) failed

Database error: lock(Array, write) failed
MySQL Error 1044 (Access denied for user '@localhost' to database 'groupware')
Function: db::halt / db::lock / config::save_repository / sessions::sessions_ / session_sessions / createobject / include / include
session halted

Compruebe los permisos de la base de datos. Su usuario no tiene los privilegios suficientes.

9.4 Comprobar los permisos de los ficheros

Este error ocurre cuando ejecuto el script de comprobación de la instalación:

Comprobando los permisos de ./phpgwapi/images para que no sea de escritura para todos: hri/users
drwx---rwx
./phpgwapi/images puede escribir en el todo el mundo!!!

Cambie los permisos en el directorio phpgwapi/images para que no sea de escritura por todos:

chmod 700 images

9.5 No puedo pasar de la página de Comprobar la instalación (1)

No hay avisos ni errores..... Instalo el fichero header.inc.php con todos los valores correctos, etc., pero acabo siempre en esta misma página check_install.php...

Compruebe que el servidor web tenga los permisos de lectura para el fichero header.inc.php y que esté en la raíz del servidor web.

9.6 No puedo pasar de la página de Comprobar la instalación (2)

Hemos instalado eGroupWare en un servidor Linux que también tiene instalado un servidor proxy.

Los clients Microsoft Internet Explorer, con una referencia al servidor proxy, aunque el servidor proxy tiene que ser ignorado (opciones->conexión->proxy->configuración avanzada).

No podemos subir adjuntos que tengan más de 1 Mb. Se ha mirado todo en los ficheros php.ini y httpd.conf, pero seguimos sin poder subir ficheros mayores de 1 MB

Es frecuente que los servidores proxy estén configurados para permitir un cierto flujo para no permitir ciertos tamaños predeterminados. Por ejemplo, en Squid, hay que cambiar el valor predeterminado del parámetro "request_body_max_size" que es de 1MB.

P. ej: request_body_max_size 20 MB

9.7 [WINDOWS] fudforum/3814******9): Permiso denegado

Warning: mkdir(D:\Websites\yourwebsite\egroupware\fudforum/3814******9): Permission denied in D:\Websites \egroupware\fudforum\setup\default_records.inc.php on line 114

ERROR: Failed to create D:\Websites\yourwebsite\egroupware\fudforum/38145******, please create this directory manually and chmod it 777SiteMgr demo site installed

Simplemente entré y creé el directorio 3814****** en el directorio D:\Websites\yourwebsite\egroupware\fudforum y le di permisos de lectura y escritura- Por favor, tenga en cuenta que el número "3814******" será el CRC32 de nuestro dominio, por lo que será distinto en cada máquina."

**Tomado del fichero D:\websites\yourwebsite\fudforum\setup\readme – "El fichero \fudforum\setup\index.php necesitará crear varios ficheros dentro del directorio navegable fudforum\. Esto necesita que se le otorguen permisos de escritura al servidor web a varios ficheros y directorios (el instalador se quejará si no fuera así). La solución más sencilla es dar temporalmente al directorio fudforum/ acceso completo y luego restaurar los permisos a los normales (lectura y escritura) cuando acabe el proceso de instalación. Si desea ahorrar unos pocos megabytes de espacio, una vez que el fudforum esté instalado, puede borrar el directorio base/, que ya no se necesita."

9.8 Sitemgr: mkdir(./sitemgr-link): Permiso denegado

Warning: mkdir(./sitemgr-link): Permission denied in D:\Websites\calvarycentral\egrouptest\egroupware\sitemgr\setup\default_records.inc.php on line 165

Can't mkdir(./sitemgr-link) !!!sitemgr/sitemgr-link copied to eGroupWare dir and sitemgr-link NOT installed, you need to copy it from egroupware/sitemgr/sitemgr-link to egroupware/sitemgr-link and install

Copie el directorio sitemgr-link de \egroupware\sitemgr\ que fue creado por eGroupWare y colocado en el directorio raíz D:\Websites\yourwebsite\egroupware. Esto le permite instalarlo desde el enlace "Administrar Aplicaciones" en la página egroupware/setup/index.php page.

10 Mapa de Software

AIDE, Advanced Intrusion Detection System

Platform	Linux / BSD / *nix
License	GPL
Homepage	http://sourceforge.net/projects/aide/
Download	
RPM	Take a look at your distribution
DEB	Debian Project
tar.gz	AIDE Project file server

Apache Web server project

Platform	Linux / BSD / Win / other
License	Apache Software License
Homepage	httpd.apache.org
Download	
RPM	Take a look at your distribution
DEB	Debian Project
tar.gz	Apache Project file server
Win	Apache Project file server

chkrootkit project

Platform	Linux / BSD
License	BSD-Like
Homepage	www.chkrootkit.org
Download	
RPM	creativix chkrootkit page
tar.gz	chkrootkit project

eGroupWare project

Platform	Linux / BSD / WIN / other
License	GPL
Homepage	www.egroupware.org
Download	
RPM	sourceforge.net eGroupWare project
tar.gz	sourceforge.net eGroupWare project
tar.bz2	sourceforge.net eGroupWare project
zip	sourceforge.net eGroupWare project

logwatch project

Platform	Linux / BSD/ other
License	GPL
Homepage	www.logwatch.org
Download	
RPM	logwatch project
tar.gz	logwatch project

logcheck project

Platform	Linux / BSD/ other
License	GPL
Homepage	sourceforge project page
Download	
tar.gz	logcheck project

ModSecurity

Platform	Linux / BSD / WIN / other
License	GPL
Homepage	http://www.modsecurity.org/
Download	
tar.gz	ModSecurity project
zip	ModSecurity project

NMAP

Platform	Linux / BSD / WIN / other
License	GPL
Homepage	http://www.nmap.org/
Download	
RPM	NMAP project
tar.gz	NMAP project
tar.bz2	NMAP project
zip	NMAP project

openssh project

Platform	Linux / BSD
License	GPL
Homepage	www.openssh.org
Download	
RPM	OpenBSD project fileserver
tar.gz	OpenBSD project fileserver

php project

Platform	Linux / BSD / WIN /other

License	The PHP License
Homepage	www.php.net
Download	
RPM	Take a look at your distribution
tar.gz	php project
tar.bz2	php project
zip	php project

Roxen web server project

Platform	Linux / BSD /WIN / other
License	GPL
Homepage	http://www.roxen.com/products/web_server/
Download	

The Linux package will be installed with a shell script

Turck MMCache

Platform	Linux / BSD / Win / other
License	GPL
Homepage	sourceforge.net/projects/turck-mmcache
Download	
tar.gz	turck-mmcache project
tar.bz2	turck-mmcache project
zip	turck-mmcache project

11 Tareas pendientes y registro de cambios

11.1 La lista de tareas pendientes de este documento

Para la versión 1.0 del documento:

- Planificación previa para una instalación de eGroupWare.
- Entrenar a los usuarios.
- Instalación de un servidor LDAP y configuración de OpenLDAP / Email / SMTP bajo *nix.
- Instalación de un cortafuegos básico bajo Linux para eGroupWare.

Más después de esta versión:

- mod_log_forensic para Apache.
- Ocultar la versión de ssh.
- Soporte para Fedora (YUM, RPM-apt).
- Añadir psad al security HOWTO.
- Instalación y configuración de sXad.
- Crear una lista de copia de seguridad recuperación ante desastres/HOWTO.
- Rsnapshot.
- Bastille Linux / LSAD.

11.2 Registro de cambios para este documento

* Sun Feb 22 2004 Reiner Jung <r.jung AT creativix DOT net> 0.4
- Cambio de licencia a creative commons
- Construir paquetes de SuSE desde source RPM
- Seguridad y optimización para Apache
- Cifrado SQL posible para la contraseña del usuario
- La instalación proporciona prefijos de cuenta para instalaciones LDAP
- Seleccionar en la instalación nombres de usuarios con mayúsculas y minúsculas
- Añadida sección de resolución de problemas
- Seguridad en eGroupWare con ModSecurity
- Actualizar el fichero header.inc.php file
- Instalación de PHP segura actualizada
  restrocción open basedir
  desactivar el registro de errores
- Instalación de Advanced Intrusion Detection System
- Cambiar el nombre Quick install HOWTO a Express Install HOWTO y extenderlo
- Express Install ahora incluye Windows
- Instalar analizador de ficheros de registro (logcheck)
- Extensión de Turck-mmcache
  Cómo instalar mmcache en RedHat Enterprise Linux
  Requisitos para instalar mmcache

* Sun Nov 22 2003 Reiner Jung <r.jung AT creativix DOT net> 0.3
- Update eGroupWare
    update with packages
    update from CVS
- Install from a RPM to a other path like /var/www/html
- Software Map
    add the software and the license from all pieces from 003 document
- some typo errors fixes
    GPG key typo fixed
- Verify the GPG key added
- Create a https certificate
- Secure PHP installation

* Fri Sep 16 2003 Reiner Jung <r.jung AT creativix DOT net> 0.2
- some typo errors fixed
    fix error in CVS install documentation
    fix type In nmcache
- chkrootkit how to added
    Checkrootkit sample snippet
    Install check rootkit RPM
    Install check rootkit tar.gz
- check your server for unneeded service / open ports
    Ports which eGW server needs to run
    The portscanner
    Output from the portscanner
    Disable unneeded services/servers
- uninstall unneeded software extended
- secure administration (ssh/sshd)
    Connecting your server with a secure session
    Working with ssh key pairs
        Creating a secure shell key pair
        Copying your public key to the server
        The ssh-add tool
        Securing your ssh client
        Securing your sshd

* Fri Sep 12 2003 Reiner Jung <r.jung AT creativix DOT net> 0.1
- Initial creation of this document

12 Colaboradores en este documento

Las siguientes personas han colaborado en este Manual de Instalación y seguridad:

Traducciones

Brasil (portugués):	Roger de Souza Moraes
Francés:	Patrice Lallement
Alemán:	Wolfgang Baumgartner, Andreas Wengrzik
Español:	Oscar Manuel Gómez Senovilla
Chino tradicional:	Finjon Kiang

Prueba de lectura

Inglés:	Jeff Mitchell (v0.4)
	Geltmar von Buxhoeveden (v0.3)

Co-Autores

Versión Windows	John W. Brown

13 Licencia legible por humanos

Attribution-ShareAlike 1.0

Usted tiene la libertad para:

- copiar, distribuir, mostrar y hacer funcionar el trabajo
- hacer trabajos derivados
- hacer uso comercial del trabajo

Bajo las siguientes condiciones:

Atribución. Debe proporcionar el crédito del autor original.

Volver a compartir. Si se altera, transforma o se crea a partir de este trabajo, debe distribuir el trabajo resultante solo bajo una licencia idéntica a ésta.

- Para cualquier reutilización o distribución, debe aclarar a los demás los términos de la licencia de este trabajo.
- Cualquiera de estas condiciones está sujeta a renuncia si se obtiene el permiso del autor.

El uso legítimo y otros derechos no están afectados de ninguna forma por lo mencionado arriba.

Este es un resumen de comprensión para humanos que es un resumen de- Legal Code (the full license).